El lado oscuro de la red

Misha Glenny

La nueva mafia del ciberespacio





Los beneficios de vivir en una sociedad interconectada y globalizada son incontables… Igual que los peligros. Compramos en línea, gestionamos nuestras cuentas bancarias en línea, nos relacionamos, aprendemos y trabajamos en línea. Vivimos en línea. Como consecuencia, el mundo virtual se ha convertido en un paraíso para las nuevas formas de criminalidad y en la pesadilla de las instituciones encargadas de protegernos de ellas.

¿Somos demasiado confiados al compartir en el mundo virtual lo que pensamos y creemos, todos los detalles de nuestra vida cotidiana? La respuesta está en este libro, resultado de dos años de investigación, en el que el autor de McMafia, Misha Glenny, escarba con determinación en la trastienda del cibercrimen a partir del auge y la desaparición de la web Dark Market, dedicada a la compra y venta de datos bancarios de ciudadanos de todo el mundo entre 2005 y 2008.

Tras recorrer medio mundo y entrevistarse con criminales, policías, víctimas y «hackers», Glenny desvela en este ensayo con aroma a «thriller» todos los secretos de la floreciente industria del cibercrimen, denuncia la insuficiencia de los medios policiales y la escasa implicación de las instituciones bancarias y, por encima de todo, plantea interrogantes sobre la seguridad en los tiempos de internet, convirtiendo El lado oscuro de la red en una lectura obligatoria para cualquiera que utilice un ordenador en nuestros días.

Lectulandia

Misha Glenny

El lado oscuro de la red

ePub r1.0
XcUiDi 28.04.2019

Título original: *Dark Market*
Misha Glenny, 2011
Traducción: David Paradela López

Editor digital: XcUiDi
ePub base r2.1



Para Miljan, Alexandra y Callum

PRÓLOGO

crimen@sigloXXI.com

A lo largo de su incesante lucha por la comodidad y el crecimiento económico, la humanidad ha desarrollado en un brevísimo espacio de tiempo un peligroso nivel de dependencia de los sistemas en red: en menos de dos décadas, una gran porción de las infraestructuras críticas nacionales (ICN para los iniciados) de la mayoría de los países ha pasado a estar controlada por sistemas informáticos cada vez más complejos.

Los ordenadores rigen buena parte de nuestras vidas, del mismo modo que regulan nuestras comunicaciones, nuestros vehículos, nuestras relaciones comerciales y con el Estado, nuestro trabajo, nuestro ocio, todo. En uno de los varios juicios por delitos informáticos a los que he asistido en los últimos años, la fiscalía de la Corona británica solicitó una orden preventiva contra un *hacker*. La orden debía entrar en vigor tras la salida de prisión del reo y tenía como fin limitar su acceso a internet a una hora a la semana bajo la supervisión de un agente de policía. «Cuando mi cliente haya cumplido la pena —observó el abogado del acusado durante la vista—, no quedará una sola ocupación humana que no esté, de una forma u otra, mediatizada por internet. ¿Cómo va a llevar mi cliente una vida normal en esas circunstancias?», se preguntaba retóricamente.

Razón no le faltaba. Por regla general, cuando nos olvidamos el teléfono móvil en casa, ni que sea por unas pocas horas, sentimos una intensa irritación y una sensación de ausencia que, entre los usuarios con mayor grado de dependencia, puede derivar en ansiedad. Lo curioso es que, cuando nos privamos del aparato por unos días, esa corrosiva sensación de incomodidad se ve sustituida a menudo por un sentimiento de liberación al vernos devueltos a un mundo, no tan lejano, en el que ni teníamos ni necesitábamos teléfonos móviles y en el que organizábamos nuestras vidas sin ellos. Hoy en día, la mayoría de las personas se creen incapaces de vivir sin esas pequeñas computadoras portátiles.

Tal vez el símil más próximo a los ordenadores sea el de los vehículos de motor. Cuando los coches se convirtieron en bien familiar de uso corriente a partir de la década de 1940, solo un reducido número de conductores conocía el funcionamiento de un motor. No obstante, no pocos de ellos eran capaces de reparar su vehículo fuera cual fuese la causa de la avería. Aún más, sabían cómo manipular un carburador para llegar hasta casa y la mayoría se las habría apañado al menos para cambiar un neumático pinchado.

En la actualidad, si se trata tan solo de un pinchazo, todavía cabe la posibilidad de que lleguemos a nuestro destino. Sin embargo, las averías son, cada vez más, el resultado de fallos del ordenador, la caja de plástico negro que generalmente se encuentra detrás del motor. Si ese es el caso, ni siquiera un mecánico de tanques experimentado será capaz de poner el coche en marcha. Con un poco de suerte, un ingeniero informático podrá repararlo, pero en la mayoría de casos será necesario reemplazar la unidad.

Los sistemas informáticos son mucho más complejos y frágiles que los motores de combustión interna, por lo que solo una exigua minoría de personas son capaces de abordar el problema, más allá del consabido mantra: «¿Has intentado reiniciarlo?».

Nos encontramos en estos momentos en una situación en que una minúscula élite (llámeselos *geeks, frikis, hackers*, piratas, segurócratas o como se quiera) posee un conocimiento profundo de la tecnología —cuya influencia en nuestras vidas es cada día mayor en fuerza y extensión—, mientras que el resto de nosotros no tenemos la más remota idea de nada. Caí por primera vez en la cuenta de este hecho durante la investigación de *McMafia*, mi anterior libro sobre el crimen organizado global. Viajé a Brasil con el propósito de investigar el tema de los delitos informáticos, porque ese fascinante país, pese a sus muchas virtudes, es uno de los principales núcleos de malas prácticas en la web, aunque por entonces casi nadie lo sabía.

Ahí conocí a unos ciberladrones que habían ideado un método de *phishing* de una eficacia extraordinaria. El *phishing* sigue siendo uno de los pilares de la delincuencia en internet. Existen dos modalidades básicas. En una, la víctima abre un correo basura. El archivo adjunto contiene un virus que permite que otro ordenador, situado en cualquier lugar del mundo, pase a controlar la actividad del ordenador infectado, incluida la introducción de claves bancarias. El otro método consiste en redactar un mensaje de correo que parezca enviado por un banco u otra institución en el cual se solicite la confirmación del nombre de usuario y la contraseña. Si el receptor pica, el pirata puede utilizar sus datos para acceder a algunas o todas sus cuentas de

internet. Los *hackers* brasileños me enseñaron paso a paso cómo se habían embolsado decenas de millones de dólares procedentes de cuentas bancarias de Brasil, España, Portugal, Reino Unido y Estados Unidos.

A continuación, visité la brigada informática de Brasilia, que había detenido a cuatro miembros de ese mismo grupo criminal (si bien la policía no dio nunca con la pista de al menos otros ocho), y más tarde me entrevisté con el jefe de la X-Force, el departamento de operaciones encubiertas de la compañía de seguridad informática estadounidense ISS. En el transcurso de una semana me di cuenta de que el crimen organizado convencional o tradicional, por pintoresco y variado que pueda ser, comporta riesgos mucho mayores que la delincuencia cibernética.

Los grupos criminales de la vieja escuela, apegados a los medios y tecnologías del siglo XX, deben superar dos importantes obstáculos si pretenden prosperar. La policía es la principal amenaza para su negocio. La eficacia de las fuerzas de seguridad varía en función del lugar y el momento. Los grupos criminales organizados se adaptan a esas variables y eligen cómo interactuar con las fuerzas de la ley y el orden: enfrentándose a ellas, sobornándolas, corrompiendo a los políticos con autoridad sobre la policía o evitando ser detectados.

Pero existe un segundo problema: las amenazas derivadas de la competencia, los piratas que como ellos surcan las aguas a la caza y captura de una presa. Como en el caso anterior, pueden enfrentarse a ellos, pueden sugerirles formar una alianza o pueden conformarse con dejar que los absorban.

Sin embargo, el grupo criminal no puede en ningún caso limitarse a ignorar al oponente; eso supondría el fracaso y las consecuencias podrían ser fatales. La comunicación con otras bandas criminales y con la policía es crucial para la supervivencia y el desarrollo del grupo, solo así conseguirá enviar mensajes adecuados tanto a unos como a otros.

En Brasil me di cuenta enseguida de que el hampa del siglo XXI es diferente.

Lo primero que se constata es la dificultad a la hora de identificar a quienes conspiran en la red. Las leyes que gobiernan internet son muy distintas de un país a otro. Este punto es importante porque, en general, en internet los actos delictivos se llevan a cabo desde una dirección IP (protocolo de internet, en inglés) de un país contra un particular o una corporación establecidos en un segundo país, mientras que el delito puede ser detectado (o cobrado) en un tercero. Así, por ejemplo, un agente de policía de Colombia

podría averiguar que la dirección IP desde la que se ha coordinado el ataque a un banco colombiano procede de Kazajistán, pero podría ser que en ese país tal hecho no fuera constituyente de delito, por lo que sus homólogos kazajos no tendrían base para investigar el caso.

Muchos delincuentes informáticos son lo bastante inteligentes como para investigar y aprovechar esta clase de discrepancias. «Jamás utilizo tarjetas de crédito o débito estadounidenses —me confesó uno de los mayores "tarjeteros" de Suecia—, porque al hacerlo me pondría bajo jurisdicción legal de Estados Unidos, independientemente de dónde me encontrase. Por eso solo trabajo con tarjetas europeas y canadienses. Me siento feliz y seguro porque nunca darán conmigo».

La divisoria que separa Estados Unidos de Europa y Canadá es determinante, ya que esas son las zonas donde se concentra el mayor número de víctimas de delitos informáticos. Las leyes europeas y canadienses dan mucha mayor protección a las libertades y derechos individuales en la red. Los últimos gobiernos estadounidenses han dotado a las fuerzas de seguridad de atribuciones que la mayoría de los países europeos nunca admitirían, lo cual permite a la policía acceder con más facilidad a los datos de compañías privadas en nombre de la lucha contra el crimen y el terrorismo.

Las consecuencias son profundas y, por el momento, inescrutables. Las consideraciones acerca del crimen, de la vigilancia, la privacidad, la recopilación de datos por parte de instituciones públicas y privadas, la libertad de expresión (por ejemplo Wikileaks), la facilidad de acceso a sitios web (el llamado debate de la neutralidad), las redes sociales como herramienta política y los intereses nacionales chocan de continuo en el ciberespacio.

Podría argumentarse, por ejemplo, que la omnipresencia de Google en todas las plataformas y aplicaciones vulnera los principios de la legislación antimonopolio estadounidense, y que la forma en que acumula datos personales facilita la labor de los delincuentes y supone una amenaza a las libertades civiles. A lo que Google podría contestar que la esencia de su carácter y su éxito reside en su omnipresencia en dichas plataformas y aplicaciones, y que esto, en sí mismo, favorece los intereses comerciales y de seguridad de Estados Unidos. Si lo desea, el gobierno estadounidense puede acceder por medios legales a los datos de Google en cuestión de horas y, puesto que Google recaba datos en todo el mundo, esto confiere a Washington una inmensa ventaja estratégica. Muchos gobiernos desearían tener los mismos privilegios. A diferencia de China, Rusia o los países de Oriente Próximo, el gobierno norteamericano no necesita *hackear* a Google para

explorar sus secretos. Le basta con una orden judicial. ¿Vale la pena renunciar a ello en nombre de la legislación antimonopolio?

Internet es un sistema de burbujas a gran escala: apenas se ha resuelto uno de los problemas que lo afectan, enseguida surge otro, aparentemente insoluble, en un lugar distinto.

Para las fuerzas del orden, el mayor problema de todos es el anonimato. A día de hoy, cualquier usuario de internet puede disimular la localización física de un equipo, siempre y cuando cuente con los conocimientos necesarios.

Hay dos formas básicas de hacerlo: la primera cibermuralla la constituye la RPV o red privada virtual, gracias a la cual varios ordenadores pueden compartir una misma dirección IP. Lo habitual es que cada dirección IP remita a una sola máquina, pero con una RPV es posible que varios ordenadores situados en distintos lugares del planeta parezcan hallarse, por decir algo, en Botsuana.

Quienes no tengan bastante con una RPV para sentirse protegidos pueden levantar una segunda cibermuralla mediante los llamados servidores *proxy*. Un ordenador situado en las Seychelles puede utilizar un *proxy*, pongamos, en China o Guatemala. El *proxy* no revela que la IP original transmite desde las Seychelles, aunque, por si acaso, el ordenador en cuestión puede formar parte además de una RPV situada en Groenlandia.

Para proyectar tramas de este calibre se requieren conocimientos informáticos avanzados, por lo que suelen ser prerrogativa de solo dos de los colectivos involucrados en la delincuencia informática: los auténticos *hackers* y los auténticos delincuentes. Ambos son operadores privilegiados y encarnan un nuevo tipo de organización criminal, pero dentro del mundo de la delincuencia informática representan una minoría.

A su lado están los piratas de poca monta, que actúan de forma individual y obtienen sumas de dinero poco menos que despreciables; a efectos prácticos, no pasan de rateros, por eso, y dada la escasez de los recursos a disposición de las fuerzas del orden, en muchos casos no vale la pena seguirles la pista. Aunque no se molesten en recurrir a RPV ni a *proxies* ni a ningún otro sistema de enmascaramiento, sus mensajes encriptados pueden complicarle mucho la vida a la policía.

En la red pueden obtenerse de forma gratuita programas para encriptar comunicaciones escritas (e incluso voz y vídeo); tal vez el más conocido sea PGP, siglas que designan algo tan coloquial como *Pretty Good Privacy* («privacidad bastante buena»).

El encriptado es una herramienta poderosa que desempeña un importante papel en seguridad informática. Se trata de un lenguaje cifrado a base de claves generadas digitalmente cuyas permutaciones alcanzan cifras tan astronómicas que solo pueden ser reveladas si se conoce la contraseña. Hoy por hoy, los documentos encriptados son seguros, aunque la Agencia Nacional de Seguridad (NSA), el organismo de espionaje digital más potente del mundo, investiga sin cesar métodos para descifrarlos. En la cofradía del cibercrimen se rumorea ya que la NSA y sus homólogas de Canadá, Gran Bretaña, Australia y Nueva Zelanda son capaces de romper estos sistemas públicos de encriptado gracias al orwelliano sistema Echelon. Echelon, según se dice, tiene acceso a mensajes telefónicos, de correo electrónico y por satélite de cualquier parte del mundo.

Las consecuencias políticas de la codificación digital son tan inmensas que en la década de 1990 el gobierno de Estados Unidos empezó a clasificar los programas de encriptado como «armas», mientras que en Rusia el hallazgo por parte de la policía o el KGB de un solo archivo encriptado en un ordenador podía significar varios años de prisión, aunque el documento no fuera más que la lista de la compra. En un momento en que gobiernos y corporaciones atesoran cada vez más información personal acerca de sus ciudadanos o clientes, el encriptado es una de las pocas medidas defensivas con que los particulares todavía pueden garantizar su privacidad. Al mismo tiempo, supone un instrumento precioso para quienes se dedican a desarrollar actividades criminales en la red.

De la misma manera que los delincuentes tradicionales crean jergas para identificar a sus amigos, enemigos, policías o rivales, los cibervillanos se enfrentan permanentemente al reto de evaluar las credenciales de autenticidad de las personas con quienes chatean en la red. Parte de este libro explica cómo han desarrollado sus métodos de identificación y cómo las fuerzas de policía de todo el mundo han intentado contrarrestar la habilidad de los *hackers* para distinguir a las autoridades y a los llamados confidentes en la red.

En la década de 1990, la forma más sencilla de evitar que individuos no deseados interfirieran en la actividad criminal pasaba por introducir un rígido sistema de veto y de aceptación de miembros en las webs dedicadas al debate de operaciones ilícitas en internet. A pesar de esas medidas de seguridad, era cuestión de meses que el Servicio Secreto estadounidense o agencias de inteligencia como el FSB, sucesor del KGB, navegaran sin problemas por esas páginas, a las que accedían fingiéndose delincuentes o captando confidentes que trabajasen para ellos.

La actuación de ciertos agentes fue tan convincente que algunas agencias de seguridad llegaron a perseguir a policías infiltrados de otros países, al confundirlos con delincuentes reales.

Fruto de esta dedicación, las fuerzas policiales y de espionaje han elaborado, a lo largo de la última década, una nutrida base de datos de *hackers* criminales: en ella constan sus alias, sus lugares de residencia verdaderos o supuestos, los tipos de actividades a las que se dedican y las personas con las que se comunican más a menudo. Los datos de los ciberdelincuentes de nivel inferior están muy difundidos. Sin embargo, a pesar de toda esta información, sigue siendo extremadamente difícil procesar a criminales informáticos.

En este punto es donde la propia naturaleza de la red —en especial sus interconexiones— crea enormes dolores de cabeza a las fuerzas de la ley y el orden: nadie puede estar cien por cien seguro de con quién se comunica en la red. ¿Se trata de un *hacker* normal y corriente? ¿O de alguien con amigos en las altas esferas? ¿Será un criminal? ¿Quizá un secreta? ¿O un investigador militar que trabaja evaluando las técnicas delictivas de los *hackers*? ¿Estamos viendo a nuestro interlocutor o es él quien nos ve a nosotros? El dinero que gana, ¿lo quiere para sí o para Al Qaeda?

«Es como una partida de ajedrez en siete dimensiones —ha observado el futurólogo Bruno Guissani— en la que nunca sabes quién es tu oponente en un momento dado».

La llegada al cuartel general de Google en Mountain View, California, no fue como ver el Taj Mahal por primera vez, pero aun así sentí un espasmo de sobrecogimiento al aparcar en la avenida Charleston, frente al letrero multicolor que anuncia una de las maravillas del mundo posindustrial.

La velocidad a la que Google se ha fundido con nuestra conciencia, con todos los pros y contras que asociamos con las sustancias narcóticas, no tiene precedentes. Sus únicos rivales son sus primos en la familia de los mastodontes digitales, como Facebook, Microsoft y Amazon. Pero ni siquiera estos pueden presumir del éxito de Google, que facilita, guía y observa nuestras vidas cada vez que sus tenebrosos servidores escupen tropecientos *bytes* de información solicitada, al tiempo que sorben y almacenan perfiles de datos individuales y colectivos relativos a miles de millones de seres humanos. Estos datos nos describen mejor de lo que nosotros mismos creemos. Solemos encogernos de hombros cuando nos preguntan qué pasaría si esa información cayera en malas manos. Puede que eso ya haya ocurrido…

La alegre mezcla de colores primarios y secundarios que conforma el familiar logo de Google se repite por todo el campus. Muchos de los voluminosos objetos esparcidos con escrupuloso desorden por el lugar tienen los bordes suaves y redondeados. Las esculturas están diseñadas para poder sentarse encima, contemplarlas o jugar con ellas, de tal modo que el complejo en su conjunto recuerda a una enorme guardería o, según el nivel de ansiedad y paranoia de cada cual, a la estrambótica ciudad de juguete de *The Prisoner* (la serie televisiva de la década de 1960), donde iba a parar todo aquel que amenazaba la seguridad del país y de la cual no había escapatoria. ¿Es mi imaginación o aquí todo el mundo, desde el personal de limpieza hasta el de dirección, sonríe como si estuviera en trance? Esto refuerza la interpretación paranoica de la esencia de Google y hace pensar que quizá exageran en lo de no parecer los malos de la película. No acabo de saber si estoy en un sueño o en una pesadilla.

Casi suspiro de alivio cuando me encuentro con Corey Louie, director de Confianza y Seguridad de Google, porque la gente que se ocupa de asuntos de seguridad suele ser seria y con cierta tendencia al secretismo, trabaje para quien trabaje. Su conducta se agradece como contraste con el aire de homogeneidad budista que se respira en Google. Louie, un elegante asiático norteamericano sobre la treintena y de maneras bruscas aunque afables, se curtió en el mundo cibernético no de la mano de los lotófagos de Silicon Valley, sino del Servicio Secreto estadounidense, en un entorno mucho más áspero y masculino. Google lo había contratado dos años y medio antes de mi visita, a finales de 2006. En el momento de abandonar las fuerzas de la ley, Corey Louie tenía a su cargo la Unidad de Crímenes Electrónicos del Servicio Secreto. Lo sabía casi todo sobre ataques a redes (las llamadas intrusiones o penetraciones), fraudes con tarjeta de crédito, los omnipresentes ataques distribuidos de denegación de servicio o DDoS (capaces de deshabilitar redes y sitios web) y el *malware*, que poco después del cambio de milenio empezó a extenderse como una plaga de ratas. También sabía mucho sobre tráfico de tarjetas, el pan de cada día en su campo. El tráfico de tarjetas consiste en la compraventa de datos de tarjetas de crédito robadas o pirateadas. Su número asciende a cientos de miles en todo el mundo, y se utilizan para comprar bienes o retirar metálico en cajeros.

¿Cómo podía Google resistirse a una baza estratégica como Corey Louie? De hecho, no pudo. ¿Y cómo podía Louie resistirse a un estratégico cambio de carrera en Google? La brisa balsámica de la costa pacífica del sur de Estados Unidos frente a la humedad de Washington, el gélido invierno y una

única semana para ver los cerezos en flor; la vestimenta informal de la Costa Oeste frente a los rígidos cuellos de la capital; el dinero y la sensación de participar en un proyecto dinámico frente a la monotonía del trabajo para el gobierno. No había color.

Circulando por la autopista 101 desde San Francisco, el viajero pasa por delante de otros iconos cibernéticos aparte de Google: Sun Microsystems, Yahoo! y McAfee se cuentan entre los muchos nombres famosos cuyo cuartel general se desliza ante las ventanillas de camino al sur. En todas las compañías que uno visita para tratar asuntos de seguridad, aparecen exagentes del gobierno provenientes del FBI, el Servicio Secreto, la CIA, la DEA (la Administración para el Cumplimiento de las Leyes contra la Droga) y el Servicio de Inspección Postal estadounidense. Falanges enteras de antiguos agentes secretos han emigrado de los asépticos alrededores de Washington para darse a la buena vida en Silicon Valley, seducidos por unas condiciones tan jugosas como las que llevaron el cine a Hollywood.

Este flujo de los organismos estatales hacia el sector privado resulta en un claro déficit para el gobierno. El Tesoro dedica fondos a formar ciberinvestigadores que, en cuanto tienen unos años de experiencia, se trasladan a climas más plácidos. La inversión no cae del todo en saco roto, pues gracias a ella se han consolidado los vínculos entre los sectores público y privado. Google no solo es una corporación privada; a ojos de la Casa Blanca, es un activo nacional estratégico. El mensaje de Washington es claro: atacad a Google y estaréis atacando a Estados Unidos. En ese contexto, que alguien como Corey Louie pueda descolgar el teléfono para llamar a sus antiguos colegas del Servicio Secreto y avisarles, por ejemplo, de que ha habido un ataque masivo contra Gmail hace que la colaboración, tan vital, entre los sectores privado y público en el campo de la seguridad en internet sea mucho más ágil.

Lo ignoro, pero apuesto a que el nivel de vida de Corey ha mejorado desde que se mudó al Oeste, claro que a cambio de trabajar muy duro. Google es uno de los dos mayores depósitos de datos del mundo; el otro es Facebook. Eso es lo que los convierte en negocios lucrativos (los anunciantes no dudan en pagar por conocer los hábitos personales que esos datos reflejan) y lo que hace que tanto los *hackers* que trabajan por cuenta propia como los que actúan en nombre de las mafias, de la industria o de los Estados rivales los codicien como si fueran el Santo Grial.

Hacia el final de nuestra conversación, Corey me habló de un amigo suyo, policía, que durante mucho tiempo se había dedicado a confraternizar con

hackers. Lo había hecho tan bien que había logrado convertirse en administrador de un importantísimo sitio web ilegal. «Imagino que le encantaría hablar contigo —dijo—. Gestionaba una web que se llamaba Dark Market». Era la primera vez que oía hablar de la web y del agente especial del FBI Keith J. Mularski. Me encontraba al principio de un extraño viaje.

Aunque se hallaban repartidos por una docena de países, decidí conocer y entrevistarme con el mayor número posible de protagonistas de la historia de Dark Market: ladrones, policías, agentes dobles, abogados, *hackers*, *crackers* y vulgares delincuentes. Consulté asimismo una cantidad ingente de documentos judiciales relativos a Dark Market y las personas involucradas en el caso. Delincuentes informáticos retirados o en activo y agentes de policía me suministraron documentación e información adicional. No pude acceder a ningún archivo completo de la web, pero conseguí examinar partes significativas. De todas las personas a las que he conocido, el agente Mularski, que posee el archivo casi íntegro de Dark Market, es la única que ha tenido acceso total a la documentación.

Aparte de ese archivo escurridizo, algunas de las pruebas documentales —aunque útiles— se revelaron inexactas; me refiero sobre todo al material aportado por la fiscalía en muchos de los juicios. A mi entender, dichas inexactitudes no fueron fruto de la incuria o el afán de venganza, ni tampoco fueron intencionadas, sino que más bien reflejaban la naturaleza extremadamente técnica y a menudo confusa de las pruebas de los juicios relacionados con la informática. La primera vez que tuvieron que afrontar un caso de delitos en la red, jueces y letrados tuvieron los mismos problemas que cualquiera de nosotros para comprender el medio.

Así pues, el núcleo de la historia remite a los personajes y a sus acciones. Por consiguiente, el testimonio que aquí se presenta se basa en buena medida en recuerdos personales que abarcan más de una década. Aparte de la consabida falibilidad del recuerdo, todos los actores implicados tenían intereses que defender, y para ello intentaron destacar determinadas facetas de la actividad de Dark Market y ocultar otras. En este sentido, se vieron beneficiados por la naturaleza ambigua de la comunicación vía internet, un medio tolerante con la mentira y el disimulo.

Mis intentos de dilucidar quién mentía, exageraba, inventaba o contaba la pura verdad triunfaron solo en parte. Todos los entrevistados eran personas de una inteligencia extraordinaria, si bien algunos carecían de la fuerza moral necesaria para mantenerse a flote en las procelosas aguas de la ciberdelincuencia. Sin embargo, a medida que escarbaba más y más en el

extraño mundo de Dark Market, caí en la cuenta de que las distintas versiones que circulaban acerca de la historia de la web eran contradictorias e irreconciliables. Ha sido imposible establecer con certeza cuál fue la verdadera relación entre los implicados y quiénes eran en última instancia sus colaboradores.

Internet ha generado cantidades abrumadoras de información, de la cual un tanto por ciento considerable es inútil, otro tanto por ciento no ha sido interpretada y una pequeña parte es peligrosamente falsa. Dada nuestra creciente dependencia de los sistemas en red y la interconectividad gracias a la cual grupos altamente especializados, como los *hackers* y los agentes de inteligencia, se mueven entre la delincuencia, el espionaje industrial y la guerra informática, reviste una importancia intelectual y social de primer orden documentar e intentar comprender la historia de fenómenos como Dark Market, aun cuando las pruebas sean fragmentarias, tendenciosas y se hallen esparcidas tanto por el mundo real como por el virtual.

LIBRO PRIMERO

PARTE I

1

LLAMA UN INSPECTOR

Yorkshire, Inglaterra, marzo de 2008

Aquella mañana de principios de marzo de 2008, el reverendo Andrew Arun John se encontraba en un ligero estado de *shock*. No era de extrañar. No solo acababa de sobrevivir a un largo viaje desde Delhi en clase económica, sino que faltaban dos semanas para la apertura de la nueva terminal 5 de Heathrow y el aeropuerto internacional más transitado del mundo podía llegar a convertirse en un calvario para los pasajeros. Su vuelo había despegado de la India hacia las tres de la madrugada y, una vez superado el control de pasaportes y el caos de la recogida de equipajes, todavía le esperaba un viaje de cuatro horas en dirección norte hasta Yorkshire.

Al encender el teléfono móvil, el reverendo John vio que tenía un número exagerado de llamadas perdidas de su esposa. Sin darle tiempo a telefonear para preguntarle a qué venía tanto revuelo, ella volvió a llamarlo. Le explicó que la policía había telefoneado varias veces solicitando ponerse en contacto con él de manera urgente.

Desconcertado y confuso, el reverendo le espetó a su mujer que lo que decía era absurdo, aunque enseguida se arrepintió del tono de sus palabras.

Su mujer, por suerte, prefirió no hacer caso de su mal humor y, de forma clara y ordenada, le explicó que la policía quería avisarle que alguien había accedido a su cuenta corriente, que el asunto era urgente y que debía llamar al agente responsable lo antes posible.

La llamada de su esposa acabó de exasperar al reverendo; su cerebro, ya exhausto, trabajaba a marchas forzadas. «¿Quién puede haber accedido a mi cuenta corriente? —se preguntó—. ¿A qué cuenta? ¿A la que tengo aquí en Barclays? ¿A la del Standard Bank en Sudáfrica? ¿O a la del ICICI en la India? ¿Acaso a las tres? Es más: ¿qué quiere decir esto exactamente? ¿Cómo es posible que alguien acceda a mi cuenta corriente?».

Después de un vuelo tan agotador, todo aquel asunto le había provocado al reverendo un estado de ansiedad y tensión. «Ya me ocuparé de esto más

tarde, cuando esté en Bradford y haya descansado», se dijo a sí mismo.

Bradford dista trescientos veinte kilómetros del aeropuerto de Heathrow. Otros cien kilómetros al este de la ciudad se encuentra Scunthorpe, donde el pequeño equipo del sargento Chris Dawson esperaba ansioso la llamada del reverendo John. El detective empezaba a presentir que aquel caso podía convertirse en terreno pantanoso; además, se encontraba con un problema aparentemente insuperable: era incapaz de abarcarlo. Las pruebas reunidas hasta el momento incluían cientos de miles de archivos informáticos, algunos de ellos lo bastante extensos como para contener trescientas cincuenta veces las obras completas de Shakespeare. En el interior de esos documentos había una biblioteca de dimensiones planetarias repleta de cifras y mensajes en un lenguaje impenetrable para cualquiera a excepción de la reducida élite iniciada en los arcanos de la terminología de la delincuencia informática.

Es posible que el detective Dawson no supiera nada sobre esa nueva y peculiar rama de la investigación criminal, pero era un buen agente de homicidios y llevaba muchos años de servicio a sus espaldas. Entre aquella infinidad de listas y series numéricas, detectó un conjunto de datos sensibles que en condiciones normales nunca habrían podido llegar a manos de un particular.

No obstante, como muchos agentes de policía descubrieron a lo largo de la primera década del siglo XXI, una cosa era dar con una información preciosa y otra muy distinta intentar relacionarla con un delito específico.

Si el detective Dawson quería persuadir a alguno de los magistrados de la aletargada ciudad de Scunthorpe, en el estuario del Humber, de que decretase prisión preventiva contra su sospechoso, tendría que aportar pruebas que demostrasen con claridad meridiana su implicación en un delito concreto. Además, cabía la posibilidad de que el juez fuera un anciano decrépito que no supiera usar ni el mando del televisor, ya no digamos el correo electrónico. No bastaba con convencer: su acusación debía ser irrebatible y, a la vez, lo bastante simple como para que cualquiera pudiera comprenderla.

El tiempo apremiaba. El sospechoso solo podía ser retenido durante tres días y ya habían pasado dos. Entre los archivos había cifras, registros de visitas, conversaciones y a saber qué más. Dawson solo tenía pequeños retazos de pruebas.

Se quedó observando un folio A4 donde había impresas una cincuentena de palabras. Entre ellas figuraba un número de cuenta (75377983), la fecha de apertura de dicha cuenta (24 de febrero de 2006), así como el saldo (4022,81 libras). También había un nombre (Sr. A. A. John), una dirección de correo

electrónico (stpauls@legend.co.uk), una dirección física (63 St. Paul's Road, Manningham, Bradford), un nombre de usuario corporativo y, lo más importante, una contraseña (252931).

Si conseguía confirmar la identidad del titular de la cuenta, y si este declaraba no haber divulgado su contraseña de forma voluntaria, tal vez Dawson podría convencer al juez de que abriera diligencias contra el acusado y le negase la fianza. Quizá con eso el sargento ganaría el tiempo necesario para hacerse una idea de lo que tenía entre manos.

Al intentar ponerse en contacto con el señor A. A. John, Dawson había descubierto que era ministro de la Iglesia de Inglaterra y que se encontraba de viaje por la India con un grupo de niños desfavorecidos. También le habían informado que no podría hablar con él hasta que volviese de Delhi. En teoría, el reverendo llegaría pocas horas antes de que el sospechoso tuviera que ser puesto en libertad. Si no se presentaba, las arenas movedizas del caso engullirían el torrente de datos que Dawson había encontrado. Y junto con los datos, sin duda también el sospechoso se fundiría en el anonimato de su *alter ego* virtual.

Por desgracia para Dawson, el reverendo John estaba tan alterado tras la conversación telefónica con su mujer que decidió no abordar el asunto hasta llegar a su parroquia, Manningham. Tanto fue así que desconectó el teléfono móvil y se concentró en el largo trayecto desde el aeropuerto.

Pero ¿por qué estaba tan alterado?

El reverendo John, fornido y de poca estatura, era un hombre de temperamento jovial. Nacido en la linde del desierto de Thar, en Rajastán, su rostro ligeramente hexagonal solía desprender un halo radiante a través de las gafas, que le confería cierto aire profesoral. Había nacido en el seno de la minoría cristiana de la India y, tras ingresar en el sacerdocio, había trabajado durante quince años para la Iglesia anglicana de la India en Delhi.

En 1996 la Iglesia de la provincia de Sudáfrica se puso en contacto con él para que tomase a su cargo una parroquia en el municipio indio de Lenasia, cinco kilómetros al sur de Soweto, durante la transición del *apartheid* al régimen multipartidista.

El cambio habría sido un reto para cualquiera; su nuevo hogar vivía momentos delicados. La alegría con que fue recibido el fin del régimen racista se truncó al constatarse cuán profundo era el resentimiento acumulado a lo largo de los doscientos años anteriores. Forasteros como el reverendo John necesitaban sofisticadas herramientas políticas y sociales para penetrar el significado de esas tensiones y averiguar cómo contribuir a mitigarlas.

El éxito de su labor en Sudáfrica no pasó desapercibido entre la jerarquía de la Iglesia anglicana y, ochos años más tarde, el obispo de Bradford, en el condado inglés de West Yorkshire, le propuso un nuevo reto: le ofreció un puesto en Manningham, un distrito residencial próximo al centro de Bradford. El reverendo John dudó: Inglaterra siempre le había parecido un lugar inhóspito, un país marcado por el tiempo desapacible y su descontrolada expansión urbanística.

También sabía que Manningham no era precisamente un lecho de rosas. Muchos británicos veían en Bradford, y sobre todo en Manningham, un símbolo de los fallidos intentos del país por integrar a sus diversos grupos étnicos y religiosos. Otros, menos benévolos, veían en Manningham una oportunidad de sembrar discordia entre las distintas comunidades.

En julio de 2001, habían estallado en el barrio breves pero violentos disturbios que evidenciaron un distanciamiento creciente entre la numerosa comunidad asiática y la población blanca. Manningham ya había experimentado el fenómeno de la emigración blanca, y en el momento de la llegada del reverendo John, tres años después de los altercados, el 75 por ciento de la población era musulmana, en gran parte originaria de los distritos rurales del norte de Pakistán. «El 25 por ciento restante son cristianos, aunque solo un 5 por ciento acude a la iglesia. Aquí, la comunidad blanca se percibe como la minoría que es», afirma el reverendo John. Aunque el clima, la arquitectura y la cultura no guardaban parecido alguno con las barriadas de Johannesburgo, en otros aspectos Manningham se asemejaba asombrosamente a Sudáfrica.

Era un destino difícil. Cuando las nubes se juntaban o empezaba a nevar, casi nada se podía hacer en aquellas calles flanqueadas por sombríos edificios neogóticos. Poco más de un siglo antes, Manningham había sido una zona en la que todo el mundo deseaba vivir. Fue un periodo, hoy olvidado para el resto del planeta, en que Bradford era saludada como «la capital lanera del mundo», y durante el cual fue un poderoso motor de la revolución industrial británica.

A principios del siglo XXI, sin embargo, Manningham llevaba muchos años en decadencia. La prosperidad y el empleo, antaño florecientes, hacía mucho tiempo que habían pasado a mejor vida, y su lugar lo habían ocupado las drogas, la violencia doméstica, los delitos contra el patrimonio y la prostitución. El reverendo John atendía a más gente en el centro de acogida —gente que intentaba escapar del cepo de la pobreza y del crimen— de la que acudía a su iglesia los domingos.

Siempre bajo la omnipresente amenaza del estallido de la violencia latente, el trabajo del reverendo John se desarrollaba en la primera línea de las guerras culturales, sociales y de clase de Gran Bretaña. Él, que no era de los que se achican por nada, casi siempre tenía una sonrisa a punto, fueran cuales fueran las circunstancias. Dadas las dificultades de su trabajo diario, se preguntó por qué la noticia de la intrusión en su cuenta corriente lo había exasperado tanto. Antes de nada, quería hablar con sus hijos, que sabían algo de ordenadores. Luego pensó que lo mejor era contactar sin tardanza con la policía para averiguar qué era exactamente lo que había ocurrido. «Lo único que quiero —pensó— es resolver esta historia y echarme en la cama lo antes posible».

Reacciones nerviosas como la del reverendo no son infrecuentes. La respuesta psicológica al descubrir que hemos sido víctimas de un delito informático es similar a la que experimentan quienes han sufrido un robo en su domicilio. Aunque la acción se restrinja al ciberespacio, un mundo formado por pequeños impulsos electrónicos, la sensación que se genera es de vulneración física. Y es que, si el ladrón se ha introducido en nuestra cuenta bancaria, ¿qué más puede haber descubierto en la intimidad de nuestro ordenador?

¿Se habrá apoderado de los datos de nuestro pasaporte para que un criminal o un agente de inteligencia elaboren documentación falsa? ¿Es posible que, mientras usted lee estas líneas, alguien esté examinando los correos electrónicos donde guarda información confidencial sobre un colega o empleado? ¿Habrá descubierto esos delicados mensajes subidos de tono o cualquier otro documento indiscreto que usted haya enviado o recibido? ¿Existe alguna parcela de su vida a salvo de alguien que haya obtenido acceso a su ordenador?

El reverendo John resolvió llamar al agente de policía del vecino condado de Lincolnshire nada más llegar a su acogedora casa sita junto al imponente chapitel de su iglesia de Manningham.

Que un caso como ese fuera a caer a manos de Chris Dawson, un agente de mediana edad con base en Scunthorpe, fue algo francamente insólito. La mayoría de los casos de delincuencia informática de Gran Bretaña van a parar a las unidades especializadas de tres cuerpos: la policía metropolitana, la policía de la ciudad de Londres y la Agencia contra el Crimen Organizado (SOCA), también con sede en la capital. La mayor parte de los agentes sin formación específica pasan por alto ese tipo de casos debido a su esotérica naturaleza. Pero Dawson no era un agente cualquiera, sino un policía con

instinto y gran capacidad de observación. Poseía también un discreto encanto, y, como buen inglés del norte, tenía un carácter sincero que contribuía a su forma de trabajar metódica y precisa. Su buen ojo para los detalles habría de serle muy útil en los meses venideros.

Si a Manningham se la relacionaba con las tensiones étnicas y el declive económico, la cercana Scunthorpe (75 000 habitantes), al sur del estuario del Humber, era vista como un lugar anodino o como excusa para inventar chistes a propósito de su nombre o de los resultados, siempre nefastos, de su equipo de fútbol. (En justicia, hay que añadir que por lo menos no heredó el nombre escandinavo original, Skumtorp, y que, hasta su descenso en mayo de 2011, el Scunthorpe United FC plantó cara a clubes mucho más fuertes que él en la segunda división inglesa). Hasta donde alcanza nuestro conocimiento, la ciudad nunca había aparecido citada en conexión con actividades criminales a gran escala.

Solo cuatro días antes del regreso del reverendo John de su viaje de caridad por la India, el detective Dawson se encontraba trabajando tranquilamente en la comisaría central de Scunthorpe. Estaba consultando el registro de mando y control, una pantalla de ordenador donde se relacionan la información y las denuncias transmitidas por los ciudadanos. Por lo general se trata de peleas entre borrachos, de algún caso de violencia doméstica o de gatitos que no pueden bajar del árbol. Sin embargo, el miércoles a la una y media de la tarde apareció un mensaje que llamó la atención del sargento. Era un aviso fuera de lo común. Se volvió hacia su compañero y, con su cadencioso acento de Lincolnshire, le dijo: «Vámonos. Será mejor que vayamos a echar un vistazo. Parece que en Grimley Smith ocurre algo que tiene mala pinta».

2

MIRANDA ANUNCIA UN MUNDO FELIZ

La página web de Grimley Smith luce una fotografía en tonos sepia de su edificio principal tomada en época eduardiana, cuando era uno de los primeros salones de exposición y venta de automóviles de Scunthorpe. Curiosamente, el establecimiento de la foto anuncia con orgullo el Belsize, antiguo símbolo de elegancia sobre ruedas en Gran Bretaña, cuyo fabricante tuvo que liquidar el negocio poco después de la primera guerra mundial. Pero tanto este venerable antecedente como el dickensiano nombre de Grimley Smith llevan a engaño, ya que GSA, como también se la conoce, no fue fundada hasta 1992 por cierto señor Grimley y cierto señor Smith.

Los servicios técnicos que ofrece la compañía son mucho más complejos que la venta y reparación de viejas carracas. La empresa está especializada en aplicaciones de ingeniería química destinadas a la industria energética y farmacéutica, y se cuenta entre las jóvenes compañías de Scunthorpe con mayor éxito y presencia internacional.

Al principio, la plantilla de GSA la formaban tan solo sus dos fundadores, pero desde entonces se ha expandido y hoy en día da trabajo a varias docenas de ingenieros altamente cualificados. Como todos los negocios en que éxito equivale a expansión, GSA creció de forma prometedora pero anárquica. Sus ingenieros conseguían contratos para participar en proyectos titánicos en lugares tan lejanos como Irán, China y Venezuela. La naturaleza especializada de su trabajo y la necesidad de realizar cálculos sin margen de error exigían la utilización de potentes programas informáticos. En especial, los llamados programas de CAD (diseño asistido por ordenador), que crean simulaciones de proyectos en dos y tres dimensiones.

A mediados de 2007, la compañía había llegado a un punto en que necesitaba desesperadamente gestionar su infraestructura informática. La opción de externalizar el mantenimiento y la seguridad resultaba demasiado cara, pero al mismo tiempo la compañía veía cómo la gestión de sus necesidades cibernéticas cada día se complicaba más. Sus directores

decidieron que había llegado el momento de afrontar el problema de una forma distinta.

Darryl Leaning, un agradable muchacho de la ciudad, era la persona ideal para el puesto. Aparte de su competencia técnica, era joven y de una sinceridad a toda prueba. Aunque quizá lo determinante fue que, tras su carácter tranquilo y amistoso, se escondía una perspicacia prodigiosa. Con frecuencia se olvida que a un buen gestor informático se le da igual de bien gestionar expectativas sociales y psicológicas que reparar aplicaciones.

Nada más poner los pies en el despacho, Darryl constató que los ordenadores de Grimley Smith requerían atención urgente. Su principal preocupación era que todos los miembros de la plantilla poseían «privilegios de administrador» en sus terminales de trabajo. Podían instalar los programas que quisieran y utilizar todos los servicios en línea que se les antojasen (a excepción de material pornográfico, que durante la etapa anterior ya había sido bloqueado).

En los ordenadores domésticos, quien ejerce de «administrador» es una persona (por lo común, uno de los padres). Él decide, por ejemplo, si se limita la cantidad de tiempo que los demás miembros de la familia pasan delante del ordenador, o si se restringe el tipo de webs a las que pueden acceder.

Uno de los «privilegios» más importantes que los ordenadores familiares confieren al administrador tiene que ver con la instalación de nuevos programas. De este modo, los padres pueden evitar que sus hijos accedan a juegos que consideran inapropiados. Pero también pueden impedir la descarga de programas de procedencia dudosa, que podrían contener virus u otros materiales perniciosos y convertir el entorno digital de la familia en un objetivo vulnerable.

Los mismos principios rigen en un entorno de trabajo, solo que por lo común a una escala mayor o más compleja. El primer problema que identificó Darryl cuando comenzó a trabajar en Grimley Smith fue la ausencia de un administrador central. Ninguna empresa moderna, informó a los directores, podía admitir que sus trabajadores subiesen, descargasen o instalasen todo cuanto quisieran.

Les explicó que era preciso establecer un control centralizado para evitar que en un descuido alguien permitiera a los virus burlar las defensas de la red. Añadió que aquello no implicaba poner en duda la lealtad de sus empleados; la gente no instala antivirus en sus sistemas porque sospeche que sus colegas quieran infectarlos, pues en la mayoría de los casos eso no ocurre. Lo mismo, añadió, valía para la instalación de programas y todo lo demás. En una

empresa altamente especializada como GSA, la información tiene un valor incalculable. Si cae en las manos equivocadas, puede provocar la ruina de la compañía.

Darryl topó con algunos problemas en su cruzada por purgar el sistema informático de Grimley Smith de elementos de riesgo: esos invisibles huecos digitales por donde pueden introducirse gusanos, troyanos y virus de forma inadvertida. Lo primero que descubrió es que a nadie le gusta perder los privilegios de que disfruta; y, aparte de ver cuerpos desnudos contoneándose, la plantilla de GSA disfrutaba de muchos. Pese a ser un joven informático, Darryl demostró tener las ideas muy claras acerca de los procesos psicológicos asociados al uso de ordenadores. Tenía que conseguir a toda costa que los trabajadores renunciaran a sus privilegios de administradores locales y decidió que el mejor modo de lograrlo era actuando de forma gradual. Era consciente de que nadie desea renunciar a lo que tiene, pero también sabía que a todo el mundo le gusta recibir regalos.

Así pues, esperó al siguiente cambio de ordenadores para introducir las primeras restricciones. Encantados con sus flamantes y potentes máquinas, los empleados de GSA ya podían aceptar que a partir de entonces no podrían descargarse sus juegos y pasatiempos favoritos cuando les viniera en gana.

Demostrando una vez más su innato don de gentes, Darryl evitó métodos más abiertamente draconianos. Facebook se había convertido en un problema. No solo había muchos empleados que malgastaban recursos navegando por la red social a horas en que debían estar trabajando, sino que además la página se había convertido en lo que la industria de la seguridad llama un vector de ataque, un instrumento del que los creadores de virus pueden aprovecharse para propagar sus productos.

Darryl imaginó que, si vetaba Facebook, podía armarse un motín, así que, en lugar de prohibirlo, permitió acceder a él entre las doce y las dos de la tarde, horas en que la mayoría de los empleados hacían una pausa para almorzar. Al saber a qué horas utilizaban Facebook, Darryl podría realizar un mejor seguimiento de las posibles amenazas y tentativas de *hackear* el sistema y asegurarse así de que la página no ponía en peligro la seguridad de la compañía.

Paso a paso, fue introduciendo un sistema de control central relativamente sólido sin ganarse la animadversión de los empleados de Grimley Smith. El corazón del nuevo orden era un complejo programa llamado Virtual Network Computing o VNC, que no era otra cosa que el Gran Hermano particular de Grimley Smith. Si Darryl detectaba una amenaza o algo fuera de lo corriente

en la red, podía sacar al VNC de su estado de hibernación virtual para que el programa se lanzara a investigar en detalle lo que estaba ocurriendo en cualquiera de las varias docenas de ordenadores bajo su mando.

Una mañana, cuando el personal encendió los ordenadores, Darryl envió un mensaje en el que advertía a todo el mundo, del director general para abajo, que a partir de ese momento cualquiera podía verse sujeto a seguimiento por parte del programa. Con el desconocimiento de la mayoría, el nuevo VNC de Darryl los vigilaba desde un segundo plano. Si recibía la alerta de que alguien había descargado un virus o de que estaba tratando de instalar *software* desconocido, el VNC se ponía en marcha.

El VNC es una herramienta de gran potencia. A algunos, su uso puede parecerles una práctica empresarial normal y corriente, pero en internet la llegada de programas como VNC despierta críticas feroces. En buena parte de Europa continental, gobiernos y compañías tienen estrictamente prohibido acceder a la información almacenada en los ordenadores de sus empleados que no esté relacionada con el trabajo (y ni siquiera a esta es fácil acceder). La supervisión del correo electrónico constituye una ilegalidad flagrante.

La detección del crimen y las libertades civiles siempre han sido extraños compañeros de cama, pero su coexistencia se ha problematizado de forma significativa con la expansión de internet, y así seguirá siendo en el futuro. En Alemania, si un agente de policía le sigue la pista a alguien de forma anónima por internet, está obligado a identificarse como miembro de las fuerzas del orden si así se lo pide su interlocutor virtual. Esto dificulta mucho la práctica, habitual en Gran Bretaña y Estados Unidos, de utilizar a agentes que se hagan pasar por menores con el fin de atrapar a pedófilos sospechosos de captar a niños por la red. El uso del VNC tiene connotaciones políticas y está sometido a leyes sobre protección de datos. Esto significa que Darryl debía andarse con sumo cuidado a la hora de manejar su juguete.

Un día a principios de febrero de 2008, en la pantalla de Darryl apareció una alerta de *software* sospechoso: «Aplicación no autorizada: mensajería». Los sistemas de Darryl rastreaban en busca de distintos tipos de aplicaciones no autorizadas. La palabra «mensajería» sugería que alguien estaba intentando instalar o utilizar algún paquete de comunicaciones como, por ejemplo, Skype. A los pocos minutos, Darryl había descubierto que quien había disparado la alarma era uno de los ingenieros químicos que conformaban la espina dorsal de GSA. Darryl decidió llegarse hasta el puesto de trabajo en cuestión y preguntarle directamente al empleado si había puesto

en funcionamiento algún programa de mensajería instantánea desde su equipo.

«Entonces me miró con toda tranquilidad y me dijo: “¡No!”. Lo negó de forma rotunda. Así que le respondí: “De acuerdo. Aunque me parece raro, porque acabo de recibir un aviso que dice que en este ordenador se está utilizando una aplicación de mensajería no autorizada”».

Darryl se encogió de hombros. La respuesta del ingeniero tampoco lo sorprendió demasiado, ya que los sistemas de seguridad son instrumentos muy sensibles y el empleado estaba utilizando varias herramientas de escaneado que los programas de seguridad pueden confundir con incursiones de *hackers*. Sea como fuere, pensó Darryl, aunque el ingeniero hubiera estado utilizando los programas que decía, lo más probable era que estuviera chateando con sus compañeros en horario laboral. A partir de entonces, al menos, sabría que no debía hacerlo y que, si reincidía, Darryl estaría a la expectativa. El incidente, por lo tanto, quedó olvidado.

Dos semanas después, sin embargo, los hechos se repitieron. En esta ocasión, Darryl decidió despertar al temible y poderoso VNC. Tras introducirse en el ordenador del ingeniero, empezó a buscar el programa de mensajería y no tardó en averiguar que se trataba de Miranda Instant Messaging. Es mucha la gente que hoy en día utiliza la mensajería instantánea para hablar en tiempo real con las amistades mediante el envío de unas pocas palabras o frases en pequeñas cajas de texto. Las más de las veces, el programa de mensajería de Windows (Messenger) solo sirve para ponerse en contacto con usuarios que disponen del mismo programa. La ventaja de Miranda reside en el hecho de que permite comunicarse con distintos programas de mensajería instantánea. Esto lo hace muy popular entre los usuarios más obsesivos.

Antes de soltar el VNC, Darryl comprobó el disco duro del ingeniero para ver si lograba encontrar algo en concreto, pero la búsqueda resultó infructuosa. Eran alrededor de las doce y cuarto, hora del almuerzo. El momento ideal para averiguar de una vez por todas si realmente el ordenador del ingeniero estaba ejecutando el programa de marras.

Miranda no era nada en comparación con lo que Darryl encontró cuando VNC empezó a explorar las tripas del ordenador del empleado. El ingeniero había abierto diez documentos de texto al mismo tiempo y se desplazaba a través de ellos a una velocidad imposible. Darryl se quedó boquiabierto. Nunca había visto a nadie capaz de trabajar con documentos a tal velocidad. Si miraba la pantalla del ingeniero, no distinguía más que una borrosa masa

de cifras, símbolos y palabras. Poco a poco se dio cuenta de que el ingeniero estaba copiando partes del documento que, a continuación, pegaba en un archivo separado de Wordpad.

Todavía no entendía lo que estaba ocurriendo ni de dónde provenían todos aquellos documentos, pero aquello no parecía tener relación con el trabajo de la empresa. El nombre del archivo en el que estaba pegando el texto resultaba desconcertante. Se llamaba «Sierra Leona». El ingeniero, en efecto, estaba trabajando en el proyecto de una refinería de petróleo en Sierra Leona. Darryl suspiró aliviado; después de todo, quizá la operación era legítima. Solo más tarde cayó en la cuenta de por qué el ingeniero había elegido ese nombre: si alguien pasaba por delante de su ordenador, podía minimizar el archivo para que no se viera más que la barra de herramientas y una pestaña titulada «Sierra Leona», el proyecto en que trabajaba.

Darryl podía haberse llevado a engaño de no ser porque en ese momento el VNC localizó una unidad no registrada (F:), lo cual sugería que el ingeniero estaba utilizando algún tipo de memoria portátil. Darryl se introdujo en la misteriosa unidad gracias al VNC y copió las decenas de miles de documentos que encontró en su interior.

Dudoso aún acerca de cómo proceder, e incapaz por el momento de determinar qué estaba ocurriendo, Darryl ordenó a su fiel VNC que se adentrase una vez más en las tripas del ordenador bajo sospecha. Lo programó para que tomara capturas de pantalla del PC del ingeniero cada treinta segundos. Mirando la pantalla en tiempo real no había manera de entender nada; resultaba imposible averiguar qué datos eran aquellos. Sin embargo, cuando vio las capturas de pantalla —imágenes congeladas de la actividad del ingeniero—, empezó a formarse una idea de lo que estaba sucediendo: eran cientos y cientos de números de tarjetas de crédito, cuentas corrientes, detalles personales, números PIN y direcciones de correo electrónico. Aquello no tenía nada que ver con el desarrollo de la incipiente capacidad refinadora de Sierra Leona.

Acto seguido, Darryl imprimió una página particularmente densa del Bank of America y se la llevó a Mike Smith, el director general. Minutos después, Mike Smith descolgó el teléfono y llamó a la policía de Scunthorpe.

Cuando el detective Dawson se personó en Grimley Smith, el director general le mostró unas listas que contenían una cantidad de datos inverosímil: información relativa a bancos, agentes inmobiliarios, compañías de seguros, parques de atracciones, cines, organizaciones benéficas, entre otros, incluidos datos que a todas luces parecían extraídos de los archivos del ejército de

Estados Unidos. Al momento temió que se enfrentaba a algún tipo de fraude, pero no conseguía averiguar qué significaba todo ese material ni cómo confirmar su temor. La situación era espinosa.

«Muy bien —dijo Dawson—, llamémoslo al despacho para hablar con él».

Los directores de Grimley Smith intercambiaron una mirada nerviosa.

«¿Qué ocurre?», preguntó Dawson.

«Es un tipo corpulento —le respondieron—; podría resistirse».

«Bien, ya nos ocuparemos de eso cuando llegue el momento», repuso Dawson con toda la autoridad de que fue capaz.

Cuando su alta e imponente figura apareció en el despacho, el ingeniero parecía más sorprendido que furioso. Le preguntó al detective quién era y qué hacía ahí, dejando notar un atisbo de desprecio. Dawson le explicó por qué estaba en GSA y le preguntó sin rodeos para qué quería toda aquella documentación. Con inesperada indiferencia, el ingeniero contestó que formaba parte de un informe que estaba compilando para uno de los directores ahí presentes. Hubo un momento de silencio antes de que el director replicase: «¡No, eso no es cierto!».

«Muy bien —dijo Dawson—, extienda las manos, haga el favor —y haciéndole un gesto a su colega, añadió—: ¡Espóselo!».

Lejos de resistirse, como los directores habían temido, el hombre mantuvo la calma en todo momento, aunque parecía algo descolocado. Dos horas después de ver el informe de mando y control, Dawson tenía a un sospechoso bajo arresto en el calabozo. Ahora había que conseguir pruebas para presentar cargos. Si en tres días no conseguía reunir indicios razonables de conspiración o fraude, tendría que soltar al detenido y todo quedaría ahí.

Dawson regresó a Grimley Smith con un agente de la unidad de recuperación de alta tecnología y ambos se pusieron a trabajar con Darryl Leaning. Tal como Darryl había predicho, los discos portátiles contenían cientos de miles de documentos, la mayoría repletos de detalles relativos a tarjetas de crédito y cuentas bancarias pirateadas. También había correos electrónicos, algunos de ellos relacionados con un grupo de noticias de Yahoo! bautizado con el prosaico nombre de bankfraud@yahoogroups.com. Los mensajes del grupo no eran tanto un tutorial en línea como un auténtico máster sobre cómo perpetrar fraudes en la red.

Lo siguiente que hizo Dawson fue dirigirse al piso de Plimsoll Way, en la vecina Hull, donde residía el sospechoso. La dirección correspondía a una de las fincas del plan de regeneración de la zona de los muelles que empezaba a

mostrar los primeros signos de deterioro. Mugrientas manchas de agua ensuciaban la fachada de piedra de color crema, picada por el óxido que emergía de debajo del enlucido. Todo un símbolo de la Gran Bretaña del nuevo laborismo: reluciente por fuera, pero incapaz de seguir evitando que la podredumbre interna aflore a la superficie.

El domicilio era un piso de soltero en toda regla. No es que fuera una cuadra, pero sí había un poco de desorden. «Le falta un toque femenino», pensó Dawson. Al entrar en el dormitorio, el detective supo que había dado con la pista que buscaba. Sobre la cama había dos ordenadores portátiles, uno de ellos encendido. Encima, había una pila de documentos, incluidos infinidad de recibos de transferencias enviadas a (o recibidas desde) distintos lugares del mundo vía Western Union: Nueva Zelanda, México, Emiratos Árabes Unidos, Ucrania…

Resultaba muy interesante haber dado con todos aquellos archivos y documentos pero, como sabemos, lo que Dawson necesitaba eran pruebas de un delito en concreto a partir del cual presentar cargos. Al ir a tomar un montón de papeles, uno de los folios cayó flotando al suelo. A lo largo de los meses siguientes, Dawson pensó a menudo en esa serendipia. En el folio figuraban los detalles de un hombre de West Yorkshire y todos los números de sus cuentas. Después de estudiarlos, Dawson creyó que esa podía ser la prueba definitiva, pues incluía una contraseña. Si podía demostrar que esa persona no le había revelado a nadie su contraseña, tal vez podría sacar adelante el caso. Ese era el motivo por el cual el detective Dawson estaba tan ansioso por hablar con el reverendo Andrew Arun John. Si John lo confirmaba, Dawson podría acusar al sospechoso de un delito de fraude electrónico y muy probablemente el juez le denegaría la fianza. Dawson podría embarcarse entonces en la hercúlea tarea de sumergirse en aquel océano de documentos.

3

EL *MR*. HYDE DE LAGOS

En 2003 Adewale Taiwo obtuvo su licenciatura en ingeniería química por la Universidad de Lagos. Hijo de un profesor universitario y de una funcionaria, Adewale, muchacho alto y llamativo, se había convertido en un joven sensato y elocuente con un futuro prometedor en la docencia o en el sector privado. En comparación con la media nigeriana, la situación de la familia era holgada y, además, tenían parientes en Londres que podían ayudarlos en caso de que el muchacho decidiera continuar su formación en el Reino Unido.

Ese mismo año, Adewale creó su *alter ego*: Fred Brown, de Oldham, Lancashire. A pesar de que Adewale todavía no había estado nunca en Inglaterra, decidió inventarse ese auténtico *Mr*. Hyde del cibermundo. Fue Fred Brown quien creó el grupo de noticias sobre fraudes bancarios en Yahoo!

Poco después, Fred Brown empezó a colgar anuncios en internet, por medio de webs como *Hacker Magazine, Alt 2600* o *UK Finance*:

> OFERTA: Oferta de trabajo para empleados de banca o personas con familia o amigos en banca que deseen formar sociedad. Entre los bancos se incluyen el HSBC y el Royal Bank of Scotland, pero otros también serán tomados en consideración. Diríjanse a Fred B. Brown por Yahoo!, ICQ o Safemail.

Los programas de mensajería ICQ (derivado de *I seek you*, «te busco») y el más antiguo IRC (Internet Relay Chat) son algunas de las herramientas preferidas por *hackers* y *crackers*, como a veces se conoce a los *hackers* que se dedican a actividades criminales. Se trata de servicios de mensajería instantánea con los cuales se puede chatear con una o varias personas. Para los *hackers*, lo importante es que son «dinámicos», es decir que las conversaciones mantenidas a través de ellos no dejan rastro, a menos que alguien salve los diálogos ex profeso. Safemail es un sistema de correo

electrónico encriptado cuyo código es imposible de descifrar. A menos, claro, que uno logre persuadir a un juzgado israelí para que requise la información que busca, puesto que la compañía que lo posee y lo gestiona tiene su sede en Tel Aviv.

Las personas que respondieron a los anuncios de Fred Brown fueron invitadas a ingresar en el grupo bankfraud@ yahoogroups.com, los fines y la filosofía del cual eran bien claros: «Este es un grupo para la gente que no quiere trabajar en la legalidad, sino por dinero, y que está dispuesta a saltarse las reglas. En este grupo aprenderéis a defraudar a los bancos y a usurpar identidades». El hecho de que Fred se atreviera a promocionar su negocio de forma tan explícita da la medida de la presencia que las actividades fraudulentas tienen en la red. Pasarían varios años antes de que la ley diera con él, y aun así, fue gracias a la comisión de un error grave y atípico.

Los anuncios de Fred estaban pensados para atacar sus objetivos por el medio más tradicional: la vía del topo. Si uno persuade al empleado de un banco para que afane y comparta los detalles de sus clientes, se ahorra tener que piratear las cuentas o las tarjetas de crédito. Quienes se dedican al fraude por internet invierten esfuerzos considerables en localizar empleados de banca descontentos o en situación difícil, ya que disponer de un topo de confianza trabajando para ellos dispara las ganancias de manera notable. Una vez que se ha hecho con los detalles de una cuenta, el delincuente puede acceder libremente a ella por internet como si fuera suya, para después transferir el dinero a otra cuenta que tenga designada. A menos que el infractor necesite una suma significativa de forma urgente, el método de sustracción preferido consiste en extraer pequeñas cantidades a lo largo de un periodo prolongado de tiempo, de tal modo que ni el banco ni el cliente se percaten de ello.

Fred Brown, sin embargo, desarrolló un método de fraude más avanzado. Sabía cómo penetrar hasta lo más profundo del sistema bancario, donde podía realizar operaciones tales como aumentar los límites de descubierto. Aparentemente, sabía cómo modificar nombres y direcciones, y, por supuesto, robar contraseñas.

El hecho de que pusiera los cimientos de su negocio mucho antes de trasladarse al Reino Unido, demuestra la sistematicidad con que Fred enfocaba el oficio. Era reflexivo, no adoptaba conductas de riesgo ni jugaba a videojuegos. Fred Brown (alias Freddy Brown, Fred B. Brown, Freddy B, Fred B y Freddybb) veía en internet un medio fácil y sencillo para defraudar grandes cantidades de dinero a un sinnúmero de personas.

Pero antes de que Fred pudiera actuar a sus anchas por la red, su Dr. Jekyll —Adewale Taiwo— debía ocuparse de otros asuntos. El principal, su máster de ingeniería química en la Universidad de Mánchester, adonde llegó en octubre de 2005. Un mes antes de recibir el título, en mayo de 2006, abrió una cuenta en London Gold Exchange (LGE), a la cual podía transferir dinero desde cualquier banco.

LGE se dedica a comprar oro con el dinero que depositan sus clientes y, a cambio, les asigna créditos de «moneda digital». La mal llamada London Gold Exchange —con la sede en Belice y el oro depositado en Suiza— fue una de las varias instituciones que se expandieron durante la década de 1990, favorecidas por defraudadores y prestamistas. Después de traspasar sus fondos a London Gold Exchange, Taiwo los enviaba a otra institución similar, E-Gold, desde donde distribuía dinero contante por todo el mundo vía Western Union, ya fuera para blanquearlo, ya para pagar a sus colaboradores.

Como en todo lo que hacía, demostró ser meticuloso y eficiente: un estudiante sobresaliente y un malhechor de matrícula. Grimley Smith lo reclutó con muchas esperanzas poco después de que la Universidad de Mánchester le concediera el título y al mismo tiempo que la hermandad de los estafadores telemáticos daba la bienvenida a un miembro destacado.

Adewale Taiwo era un ingeniero químico plenamente capacitado. Todavía no había cumplido treinta años y ya se lo consideraba uno de los empleados más prometedores de Grimley Smith; poco después, ya se desplazaba por razones de trabajo a lugares tan distantes como China y Venezuela. Vestía bien, pero sin ostentación; su BMW encajaba con su salario y su estilo de vida. Afrontaba sus dos vidas con la misma seriedad, en parte porque su trabajo legítimo hacía las veces de tapadera de sus actividades clandestinas. Uno de los últimos lugares donde alguien buscaría a un delincuente cibernético de altos vuelos es en una respetada y exitosa empresa del sector energético, y menos entre los ingenieros más diligentes y mejor formados de la firma.

Cuando el detective Dawson empezó a calcular la magnitud del fraude cometido por Fred Brown, se quedó estupefacto. En el mejor de los casos, las pruebas consistían en unos treinta y cuatro mil archivos, algunos de ellos de hasta cien o ciento cincuenta páginas. Al poco tiempo, encontró un archivo de cien páginas plagado de números de tarjetas de crédito estadounidenses, así como los códigos de seguridad de estas y todas las contraseñas necesarias.

El detective Dawson era agente de homicidios; nadie en todo el condado de Humberside se había ocupado nunca de fraudes por internet a gran escala,

y ni él ni el otro colega que lo ayudaba podían dejar de lado su trabajo cotidiano. No sabía ni por dónde empezar. Aparte de los archivos, habían encontrado el *software* de un MSR206, probablemente el arma más importante en el arsenal de cualquier defraudador de tarjetas de crédito, los llamados «tarjeteros». Con él, el tarjetero puede «clonar» cualquier tarjeta de crédito, es decir, copiar toda la información de la banda magnética de la parte posterior y transferirla a una tarjeta en blanco con la banda magnética vacía. El MSR206 viene a ser una fábrica de moneda de uso personal.

Entre los archivos, Dawson también encontró registradores de teclas troyanos, que son al *cracker* lo que la palanqueta al ladrón de cajas fuertes. Los antiguos virus eran criaturas que nada tenían que ver con los registradores de teclas. Los primeros virus que empezaron a circular a gran escala en la década de 1990 eran obra de adolescentes y estudiantes —los llamados *script kiddies*— con ganas de demostrar su pericia como programadores anárquicos. Por desgracia, para demostrarlo no se les ocurrió otra cosa que causar molestias al mayor número posible de usuarios en todo el mundo.

Cuando un ordenador se infectaba, podían ocurrir varias cosas: que se ralentizase; que al abrir una aplicación, por ejemplo Microsoft Word, se abriera un navegador; que el equipo se apagase de forma automática, o, en el peor de los supuestos, que se destruyeran todos los datos y archivos. Circulan historias sobre escritores que perdieron manuscritos enteros por culpa de algún virus malicioso, o sobre estadísticos que vieron cómo los datos introducidos a lo largo de varios meses eran devorados ante sus propios ojos por un infame gusano digital**[1]**.

Tras el cambio de milenio, *hackers*, *crackers* y criminales empezaron a intuir que los virus, los troyanos y los gusanos podían tener usos más lucrativos. Ingeniaron el registrador de teclas, que se difundió por internet a una velocidad de vértigo. Una vez instalado en un equipo, la función de este dispositivo consiste en identificar todas y cada una de las pulsaciones del teclado. Así, cuando tecleamos «www.hsbc.co.uk» en el navegador, el programa envía esa información a su dueño o creador, que puede hallarse en cualquier parte del mundo. Si a continuación introducimos nuestra contraseña —por ejemplo «Robinhood»—, el amo del virus —en Nueva Jersey, Rostock, Lilongwe o en la Ruritania profunda— se hará con ella al instante. ¡Bingo! ¡Mi casa es su casa! O mejor: ¡Mi cuenta bancaria es su cuenta bancaria!

Así como almacenar miles de detalles de tarjetas de crédito y números de cuentas corrientes en el ordenador no es delito, tampoco lo es poseer registradores de teclas. Puede constituir un sólido indicio de actividad

criminal, pero por sí solo no es concluyente. Dawson y su colega, pues, tendrían que examinar una infinidad de archivos si aspiraban a desenmarañar aquel sinfín de hilos enredados.

Tras introducir manualmente varios miles de datos bancarios en una hoja de Excel, el agente decidió ponerse en contacto con los bancos. Suponía que serían los primeros interesados en el caso, ya que a fin de cuentas eran los sistemas de seguridad de esas entidades los que Fred Brown había burlado con tanto éxito.

Se equivocaba.

Muchas de las averiguaciones de Dawson chocaron contra un muro porque los bancos ni siquiera se molestaron en responder a sus solicitudes. La investigación estaba convirtiéndose en una carrera contrarreloj y el detective había perdido un tiempo precioso buscando en balde la colaboración de los bancos.

La actitud de la mayoría de los bancos hacia la delincuencia informática resulta ambigua. Durante la redacción de este libro, uno de los empleados de mi banco, Natwest, me llamó para preguntarme si recientemente había realizado compras en joyerías de Sofía, la capital de Bulgaria. También me preguntó si había abonado cuatro mil francos relativos a una factura de Swiss Telecom. Le dije que no. Entonces me dijo que mi Visa de Natwest se hallaba en situación de riesgo y que necesitaría otra nueva, aunque me garantizaba que la entidad había cancelado el pago de las tres mil libras gastadas de forma fraudulenta con mi tarjeta. Como a cualquiera en una situación semejante, me alivió saber que el banco no me hacía responsable de lo ocurrido.

¿Quién pone, pues, ese dinero? ¿Los bancos? No, los bancos están asegurados contra tales pérdidas. ¿La compañía aseguradora? Tampoco, porque fijan las primas a un nivel que les garantiza que no saldrán perdiendo. Entonces, por lo tanto, ¿no serán los bancos, puesto que son quienes abonan dichas primas? Pues sí, solo que los bancos recuperan el dinero mediante la introducción de comisiones adicionales que afectan a todos los consumidores. Dicho de otra manera: el fraude bancario lo paga el conjunto de los clientes del banco.

Es lógico que los bancos no quieran airear mucho este asunto. Tampoco les gusta que la gente sepa con qué frecuencia los ciberdelincuentes vulneran sus sistemas. Los periodistas jamás consiguen arrancarles la más mínima información acerca de los ciberataques que les llueven a diario. Resulta comprensible. Más difícil es disculpar sus frecuentes reticencias a colaborar con la policía en los casos en que la información llega a los tribunales. Al

negarse a admitir que sus clientes han sido víctimas de un delito informático por miedo a la competencia, los bancos favorecen de forma indirecta los intereses de los criminales.

Salta a la vista que los bancos tienen un problema: sus clientes son la parte más vulnerable de un sistema financiero interconectado. Hoy en día, incluso los *hackers* más avezados tendrían problemas para infiltrarse en los sistemas informáticos de los bancos comerciales y de inversión. Sin embargo, introducirse en los ordenadores de la mayoría de sus clientes, espiar mientras acceden a sus cuentas y jugar con su dinero es pan comido para cualquier pirata que se precie. ¿Cómo corregir los hábitos de los clientes en la red, cuando el gran gancho de la banca en línea (y de tantas de nuestras actividades en la red) es la comodidad? En la mayoría de los casos, las elaboradas medidas de seguridad que serían necesarias para acceder a esas cuentas crearían rechazo, por tediosas.

Los bancos prefieren callar acerca de la incidencia de los fraudes, en parte por motivos de competencia y en parte porque no desean que los clientes exijan volver a las prácticas de antaño. La banca electrónica supone un gran ahorro, ya que el cliente se encarga de muchas de las tareas que antes realizaban las sucursales y sus empleados. Si de pronto todo el mundo se negara a gestionar sus finanzas por internet, los bancos se verían obligados a reimplantar la extensa red de sucursales a través de las cuales prestaban sus servicios. Eso supondría un desembolso más que considerable y, como todos sabemos, los bancos se han gastado todo lo que tenían, además de cientos de miles de millones de los contribuyentes, en descabelladas operaciones especulativas y primas hinchadas hasta niveles obscenos.

Por todo ello, el detective Dawson tuvo que unir las piezas del rompecabezas con una ayuda muy limitada por parte de la hermandad bancaria. A su favor, no obstante, jugaba el hecho de que Fred Brown había cometido un par de errores significativos a la hora de urdir su red fraudulenta: a pesar de que bankfraud@yahoogroups.com estaba registrado en el Yahoo! de Estados Unidos, la dirección de correo asociada al grupo tenía la extensión yahoo.co.uk. Al tratarse de un dominio británico, Dawson pudo requerir el material a Yahoo! de manera inmediata. Menos suerte tuvo con la cuenta de Safemail. Para esta tuvo que pedir a un juzgado británico que solicitase a uno de Israel que Safemail le permitiera acceder a la cuenta encriptada de Fred Brown. El proceso se prolongó varios meses, y durante todo ese tiempo tuvo que soportar presiones por parte de los tribunales para que facilitase las pruebas a los abogados de la defensa y agilizara los trámites.

Los superiores de Dawson estaban descontentos; la presión era cada vez mayor. Los titulares de las tarjetas de crédito se hallaban repartidos por todo el mundo y ninguna de las víctimas investigadas residía en Humberside. Uno de los afectados, el reverendo John, vivía en el vecino condado de West Yorkshire, pero era el único. A Dawson le dijeron más de una vez que el cuerpo no podía permitirse destinar a uno de los mejores agentes de homicidios a un caso de fraude totalmente ajeno a su jurisdicción. Pero algo le decía al detective que valía la pena seguir adelante. Como no estaba dispuesto a arrojar la toalla, y para contentar a sus superiores, empezó a trabajar en el caso en sus horas libres, en ocasiones hasta muy tarde por la noche, intentando encontrarle sentido a aquel baile de cifras.

Desesperado por cómo la investigación sobre Adewale Taiwo estaba empezando a hacer mella en su vida, Dawson solicitó la colaboración de la unidad de inteligencia de la región. Le dijeron que no podían ayudarlo, pero le sugirieron que preguntara a la Unidad de Alta Tecnología de la Ciudad de Londres si disponían de información que pudiera serle útil. La respuesta fue negativa, pero lo remitieron a la Agencia contra el Crimen Organizado.

Finalmente, Dawson se puso en contacto con la SOCA en el cuartel de operaciones secreto del organismo en Londres, que parece sacado de una novela de Len Deighton: placas de bronce con el nombre de una compañía ficticia y una plantilla que finge no trabajar para la agencia, a la que Tony Blair describió como la réplica británica al FBI (para irritación de sus agentes).

Dawson dijo que necesitaba asistencia en un complejo caso de fraude en el que estaba involucrado un tipo misterioso que respondía al nombre de Fred Brown. La contestación telefónica de los peces gordos de la metrópoli fue seca y directa: «¿Qué sabe usted acerca de Freddie Brown?». A fin de cuentas —podía colegirse por el tono—, él no era más que un tarugo de Humberside.

«Nada —respondió el detective Dawson—, lo único que sé es que lo tengo en prisión preventiva en Scunthorpe».

Se hizo un silencio al otro lado de la línea.

«¿Alguna vez ha oído hablar de una cosa llamada Dark Market, detective Dawson?», preguntó la voz.

«No, nunca. ¿Por qué?».

Dawson había cobrado una pieza mayor de lo que creía.

La noticia cogió por sorpresa incluso a la SOCA. Llevaban años con las miras puestas en Freddybb, pero la investigación sobre Dark Market había quedado en punto muerto tras una serie de detenciones el verano anterior. Lo

último que habrían imaginado era que un policía de Scunthorpe volviera a ponerla en marcha. Pero, si algo había aprendido la mayor unidad de crímenes telemáticos de Gran Bretaña desde que en 2001 un grupo de ciberdelincuentes ucranianos abriera la primera web dedicada al crimen global, era esto: espérate lo inesperado.

PARTE II

4

LOS ARCHIVOS DE ODESA

Odesa, Ucrania, junio de 2002

Llegaban de puntos tan septentrionales como San Petersburgo y Letonia, en el mar Báltico; uno de los delegados venía de Bielorrusia, país creado en 1990 a modo de memorial viviente del comunismo. Los rusos eran mayoría, y, dentro de la propia Ucrania, habían llegado tropas de delegados de Ternopil, en el oeste; Kiev, en el centro; Járkov, en el norte, y Donetsk, en el este.

Pero el Primer Congreso Mundial de Tarjeteros (PCMT) era internacional de verdad. Algunos de los asistentes provenían de Europa occidental, mientras que otros habían aterrizado procedentes del golfo Pérsico, Canadá y Sudamérica. La nota de prensa del PCMT lamentaba que los delegados de Australia y el Sudeste Asiático no hubieran podido asistir por contratiempos en el viaje.

La organización había escogido a tres docenas de delegados de entre las cuatrocientas solicitudes recibidas. Quienes tuvieron la suerte de recibir el visto bueno sabían que el simple hecho de haber sido invitados daría alas a su reputación dentro del mundo férreamente jerarquizado de la delincuencia informática.

Para despistar a la policía, en un principio los organizadores habían anunciado que el evento se celebraría a bordo de una serie de yates de lujo amarrados frente a las costas turcas del mar Negro, pero solo era una finta. Después de todo, ¿dónde podía celebrarse el primer congreso de ciberdelincuentes sino en Odesa, la legendaria ciudad del hampa ucraniana?

El zar, Stalin y Hitler habían intentado domeñar aquella bestia con métodos de probada eficacia, pero ninguno de ellos había logrado aplastar a la hermandad criminal más resistente de Europa del Este. «La historia de Odesa es inconcebible —escribió un cronista acerca de su ciudad natal— si no se comprende la vida de sus gánsteres».

Para la mayor parte de Europa del Este, el desenfrenado capitalismo mafioso que siguió al desplome del comunismo en la década de 1990 fue un

fenómeno del todo inesperado, pero Odesa sabía lo que se avecinaba. La ciudad no tenía más opción que abrazar la nueva era, y hay que admitir que lo hizo con entusiasmo. De un día para otro, las estrellas rojas se convirtieron en luces rojas. Detrás de la avenida Primorskaya brotaron como setas sórdidas salas de juego, y poco después de 1989 los restaurantes y las saunas se convirtieron en escenarios de voracidad y derramamiento de sangre.

En los barrios de grandes bloques del extrarradio, la droga se convirtió en moneda de cambio habitual. Jóvenes sin recursos se engancharon a la *boltushka*, una mezcla casera de anfetaminas, que se pinchaban hasta provocarse cicatrices, lesiones cerebrales o incluso la muerte.

Pistoleros y clanes procedentes de Chechenia y Moscú rivalizaban con los jefes locales por hacerse con el control de la ciudad. Odesa, en teoría, formaba parte del nuevo Estado independiente de Ucrania, pero la ciudad era rusófona y, lo que es más importante, el único puerto de aguas cálidas capaz de servir de plataforma a las exportaciones rusas de gas y petróleo.

La hiperinflación y el nacionalismo hundían el rublo, el karbóvanets, la grivna o cualquiera que fuera la moneda que el gobierno proclamaba como divisa «auténtica». Lo único que proporcionaba estabilidad real era el dólar estadounidense.

Para los ciudadanos de a pie, en la década de 1990 Odesa significaba dos cosas: supervivencia y dólares. Cómo se consiguiera lo primero o se rentabilizara lo segundo no importaba. Es más, quienes lograban ambas cosas eran admirados, aunque ni siquiera amasar fortunas de un día para otro era garantía de una larga vida.

Ante ese estado de cosas, ¿quién podía culpar a Dimitri Golubov, de treinta años, por vender documentación de vehículos y permisos de conducir con la firma falsificada del director de la Oficina Municipal del Transporte? Si había hombres de negocios dispuestos a pagar por ellos, era señal de que sin duda su trabajo tenía valor real.

Tales eran las circunstancias en Odesa. Pero el joven Dimitri habitaba un mundo distinto del de las bandas tradicionales de la ciudad, centradas en la extorsión, los burdeles, el petróleo y el caviar. En vez de empuñar navajas, él prefería sumergirse en los sótanos llenos de humo donde los adolescentes convertían sus cerebros en papilla de tanto jugar al *Street Fighter*, al *Pacman* y al *Tetris*, el gran clásico ruso. En aquella cultura subterránea no se admitía más luz que la que emanaban los neones de suaves colores y los parpadeantes monitores de los ordenadores. Los cigarrillos y la Coca-Cola eran

omnipresentes, como si fueran el único alimento tolerado por un ancestral código de honor *geek*.

Dimitri disfrutaba con los videojuegos tanto como el que más, pero por encima de todo lo que le gustaba era explorar el mundo desde las confortables cafeterías de internet de Odesa. El problema era que el joven Golubov no se conformaba con navegar por las webs de lugares distantes; lo que quería era introducirse en ellas y explorarlas por dentro.

En 1999 —Golubov tenía dieciséis años—, Visa y Mastercard bloquearon el uso de sus tarjetas en los sitios web registrados en la antigua Unión Soviética. Las facturas que las empresas de internet rusas remitían a los dos gigantes crediticios eran sistemáticamente ignoradas. Sin embargo, Golubov y otros pioneros como él pronto cayeron en la cuenta de que, si extraían y replicaban por algún medio la información contenida en una tarjeta, podían retirar dinero en cajeros automáticos o adquirir por internet productos que después eran enviados a terceros países. Una opción consistía en copiar la información a partir de la propia tarjeta de crédito, aunque ello suponía la laboriosa y, por eso mismo, insatisfactoria tarea del hurto convencional. La otra opción, con mucho la mejor, era extraer la información a partir de las bases de datos de los bancos, una mina de oro en potencia.

Aunque algunos sitios web estadounidenses no admitían pedidos de la antigua Unión Soviética, sí realizaban envíos a lugares como Emiratos Árabes Unidos o Chipre, dos países que en poco tiempo se convirtieron en destino preferente de la nueva élite monetaria rusa. Así empezó una de las primeras operaciones delictivas verdaderamente globales. Un ruso robaba dinero desde Ucrania a una empresa estadounidense y lo recibía en Dubái… ¡en apenas diez minutos!

El otro gran hallazgo que marcó la pauta del «tarjeteo» como negocio fueron las clonadoras de bandas magnéticas. Las clonadoras son aparatos que leen y almacenan las bandas magnéticas de las tarjetas de crédito. Adoptan todas las formas y tamaños. Algunas son pequeños rectángulos que pueden acoplarse a un cajero automático, de tal modo que, cuando la máquina del banco lee la tarjeta de un cliente, esta es leída también por la clonadora. Otras son idénticas a los datáfonos que vemos en los establecimientos comerciales, esos con los que nos cobran los camareros o los empleados de las gasolineras. Tanto en un caso como en el otro, es posible que haya también una pequeña cámara escondida en alguna parte para grabar el número secreto del cliente (importante: tapen *siempre* el teclado cuando introduzcan su número PIN).

A estas máquinas solo se las llama «clonadoras» (*skimmers*) cuando se las utiliza para fines maliciosos; en el resto de los casos, su función es la misma que las de uso comercial. Los delincuentes pueden adquirir las clonadoras por canales comerciales ordinarios o fabricarlas ellos mismos. En su momento, las clonadoras fueron el equivalente a la máquina de vapor de James Watt al inicio de la revolución industrial. A lo largo de la década siguiente, la inmensa mayoría de las tarjetas de crédito y de los números PIN (lo que se conoce como *dumps*, «basuras», y *wholes*, «enteros») usados de forma fraudulenta habían sido clonados en cajeros automáticos y comercios de distintos lugares del mundo.

Como buen *hacker*, Dimitri enseguida vio que los sistemas de seguridad desarrollados por el incipiente sector del comercio electrónico en Estados Unidos eran primitivos y fácilmente sorteables. Nada sabemos de sus éxitos iniciales. A Dima le gustaba decir que se había hecho millonario antes de cumplir los diecisiete, pero no hay que olvidar que las mentiras están a la orden del día en internet, y, de hecho, algunos de sus colegas cuentan una versión diferente.

«Era avaricioso, embustero y un delincuente empedernido —escribió en su *blog* otro *hacker* de Odesa—. Su imagen de millonario de éxito no tenía nada que ver con la realidad».

En ese momento, Dimitri desapareció, y, con él, algunos de sus extravagantes modelos de estafa. Meses más tarde, salió de su letargo bajo el pseudónimo de Script y se convirtió en un nombre habitual en dos webs de nueva creación: Carder.org y Carder.ru. Estas no eran otra cosa que dos foros de debate donde los *hackers* rusos rumiaban cómo amasar millones de dólares, libras, yenes y euros con las tarjetas de crédito. Uno de los miembros fundadores de estas webs recuerda esas discusiones como «apáticas, discontinuas» y, en última instancia, «infructuosas».

Pero Script siguió dándole vueltas al asunto. Si existían webs para adquirir todo tipo de productos, ¿por qué no desarrollar una para el embrionario comercio de tarjetas de crédito robadas, cuentas corrientes y demás datos de interés? Sus razones para crear una página de ese tipo en la red eran de peso: Script había llegado a acumular cantidades de información tan ingentes que no disponía de tiempo ni de medios para explotarla. Lo mejor era canjear esos datos por dinero. Quería vender.

El momento era ideal. En los cinco años anteriores, internet había experimentado un desaforado aumento de la actividad comercial, posibilidad que nadie había previsto, puesto que la red había sido concebida como una

herramienta para mejorar y acelerar la comunicación, un medio para intercambiar ideas y rumores.

Amazon, eBay, Lastminute.com y otros precursores del comercio electrónico surgieron de forma casual, pero su éxito no pasó desapercibido. Miles y miles de personas se pusieron a diseñar sus propias webs. Fue uno de esos momentos, que se dan una vez por generación, en que convergen codicia y fantasía; poco después, bancos e inversores de riesgo se persuadieron de que el comercio electrónico era sinónimo de fortuna instantánea y empezaron a inyectar dinero en esas compañías, la mayoría entidades sin valor intrínseco pese a estar capitalizadas en millones, cuando no decenas de millones, de dólares. Acababa de empezar la primera gran burbuja de la era globalizada, y surgía en el campo más apropiado: el de los activos tecnológicos.

A pesar de que la mayoría de las empresas *puntocom* en realidad no eran más que pueblos Potemkin, muchas firmas consolidadas del mundo real decidieron que transferir parte de su negocio a la red podía comportar claras ventajas.

Los primeros en dar un paso al frente en este sentido fueron los bancos, ya que, como hemos visto, pensaron que, si lograban convencer a sus clientes de que realizasen los pagos y gestionasen sus cuentas en línea, podrían ahorrarse unos cuantos empleados. Los clientes más familiarizados con la red estaban casi seguros de que lo mejor era controlar en primera persona sus finanzas, cosa que internet les permitía.

Para entonces, los amos del universo, la nueva clase de los capitalistas financieros, estaban desprendiéndose de los grilletes que en el pasado habían restringido sus actividades especulativas en el mercado de derivados. Básicamente, los políticos de Washington y Londres les concedieron licencia para especular (el *boom* de las *puntocom* es un buen ejemplo). Al ver que acciones de poco valor aumentaban de precio hasta niveles desorbitados, los inversores depositaban su dinero en dichas acciones atraídos por su valor teórico. Durante una década, Occidente disfrutó de créditos bajísimos. La Edad del Imperio y el Capital se metamorfoseó en la Edad del Plástico.

A mediados de los noventa, la deuda por tarjetas de crédito personales empezó a aumentar a un ritmo implacable en los cuatro países más dependientes del dinero de plástico: Estados Unidos, Reino Unido, Japón y Canadá. En el lapso de diez años a partir de 1997, el número de tarjetas de crédito en circulación en todo el mundo ascendió de apenas mil quinientos millones a tres mil millones, y la deuda media individual entre sus usuarios más dependientes, los estadounidenses, se dobló de cinco a diez mil dólares.

Los bancos estaban encantados con nuestra nueva afición a las tarjetas de crédito porque, aunque por entonces las tasas de interés eran prácticamente del cero por ciento, ellos seguían cobrándole a todo el mundo entre un cinco y un treinta por ciento. En Gran Bretaña, el director de Barclaycard confesó ante una comisión parlamentaria que él no usaba tarjetas de crédito «porque sale demasiado caro».

Otras zonas del planeta se mostraban menos inclinadas a sucumbir al plástico. Europa occidental se había salvado en el pasado de la piratería económica que triunfaba en Estados Unidos y Gran Bretaña. Por consiguiente, el porcentaje de tarjetas de crédito era mucho menor, al igual que el nivel de deuda personal. En Europa del Este no existía ni una distribución de capital suficiente entre la población ni una industria bancaria segura capaz de administrar las tarjetas de crédito. El dinero de plástico era una rareza en el antiguo mundo comunista, un juguete para los *nuevos rusos*, el minúsculo porcentaje de población que había acaparado formidables fortunas a base de explotar a sus propios países y compatriotas durante la transición del comunismo al capitalismo.

Sin embargo, en la economía de casino anglosajona del último decenio del siglo XX y el primero del siglo XXI, el plástico era lo más parecido a una máquina de billetes inventada por las instituciones financieras, y los bancos no tardaron en explotar ese rico filón de capital. Los domicilios de todo Occidente recibían a diario toneladas de folletos en los que se exhortaba a la gente a contratar tarjetas de crédito o a canjear una deuda existente por una nueva cuenta que no rindiera intereses hasta el sexto mes. Durante tres o cuatro años, el número de diligentes consumidores que transferían sus boyantes saldos de una tarjeta a otra con crédito a interés cero no dejó de aumentar; los bancos, entretanto, vivían cada día más obsesionados con ganar nuevos clientes.

Millones de tarjetas. Dinero a espuertas para jugar. A la vista de tantos fajos de billetes electrónicos pululando por la red, acaso no deba sorprendernos que los aficionados a la informática de los países del Este —a quienes les faltaba dinero pero les sobraba ingenio— empezaran a centrar en ellos su atención. Uno de ellos era Script: Dimitri Golubov, dieciocho años, de Odesa.

He aquí cómo nació Carder Planet.

5

CARDER PLANET

Aparece, de forma gradual, una frase escrita con la tipografía de *La guerra de las galaxias*:

> ¿Buscas una solución profesional?

La imagen hace *zoom* sobre un globo terráqueo que gira a gran velocidad y que, de pronto, se convierte en un psicodélico dibujo metálico. De fondo, suena un agresivo ritmo *electrodance*. A continuación, aparecen una serie de mensajes:

> Descubre el poder de la tecnología
> ¿Harto de la rutina cotidiana?
> ¿Quieres cambiar tu estilo de vida?
> ¡Únete a nosotros!
> ¡Los dumps (tarjetas de crédito)
> pueden hacerte rico!

La pantalla funde a negro. Acto seguido aparecen tres mensajes más, reforzados por un bombo de ecos militares:

> Un equipo de confianza
> ¡Bum!
> Todo lo que necesitas para hacer negocio
> ¡Bum!
> Carder Planet es inevitable
> ¡Bum!

Un año después de la fundación de Carder Planet, en 2001, Script invitó a sus amigos *hackers* al Primer Congreso Mundial de Tarjeteros en Odesa —la primera convención de ciberdelincuentes de la historia— para celebrar la creación de su web pionera. Los miembros del grupo podían presumir de

poseer las mismas habilidades tecnológicas que los de la República Hacker, la agrupación secreta de la que formaba parte la heroína Lisbeth Salander, con el alias de Wasp, en *Los hombres que no amaban a las mujeres*, el superventas de Stieg Larsson.

Solo que Script y sus amigos no eran de ficción. Carder Planet existió de verdad.

6

ASUNTOS DE FAMILIA

El Primer Congreso Mundial de Tarjeteros conmemoró el primer aniversario de Carder Planet. Fue una ocasión única y excepcional. En 2002, Odesa se había calmado: se atisbaba incluso algún signo de normalidad. Su avenida más emblemática, Deribasovskaya, estaba repleta de vendedores ambulantes, tiendas y restaurantes de moda. Al amparo del trébol de cuatro hojas y las inscripciones gaélicas del Mick O'Neill's, uno de los primeros falsos *pubs* irlandeses de la Ucrania poscomunista, un pequeño núcleo integrado por los mejores *hackers* de Ucrania, conocido como la Familia, discutía los objetivos del congreso. Entre ellos figuraban grandes nombres como Auditor, Rayden y Bigbuyer, así como algunos de los promotores del evento: Boa, un as de las comunicaciones y la seguridad, con su característica barba blanca, y Script, un tipo enérgico aunque algo infantil.

A lo largo de los tres días siguientes, bebieron y cantaron en distintos lugares de la ciudad, pero sobre todo discutieron el desarrollo a corto y largo plazo de su joven web, Carder Planet, que ya empezaba a alterar la esencia de la delincuencia cibernética en todo el mundo.

Los debates generales tuvieron lugar en el hotel Odesa, a la sazón el más caro de la ciudad. El edificio era un bloque alto, perfecto ejemplo de la espantosa moda poscomunista, erigido justo en frente de la escalinata Potemkin, famosa por su aparición en *El acorazado Potemkin* de Eisenstein, la obra maestra del antiguo cine soviético. Uno de los temas que interesaban a todos los delegados presentes en el Odesa era la necesidad de comprender los detalles técnicos de tarjetas de crédito de categoría inferior, como JCB y Diners, que parecían marginadas en favor de las franquicias de Visa y Mastercard, más lucrativas. También se acordó crear o consolidar nuevas redes de colaboradores que pudieran «canjear» tarjetas de crédito robadas en regiones como Sudamérica, Oceanía y África. Al fin y al cabo, alguien tenía que ejecutar la parte auténticamente delictiva: retirar metálico de los cajeros. Todos convinieron en que había que externalizar ese eslabón de la cadena, el más arriesgado.

Las reuniones más secretas tenían lugar entre los quince «tarjeteros» más importantes y se celebraban en un pequeño y sórdido restaurante cerca del mar. El objetivo era animar a los delegados a abrir su propia red de franquicias regionales de Carder Planet; así sus propietarios podrían seguir ganando dinero trabajando menos.

Al principio de la reunión, uno de los delegados menos conocidos le hizo señas disimuladamente a Boa. El tipo en cuestión había realizado un barrido electrónico del restaurante y había detectado la presencia de videocámaras ocultas y aparatos de grabación digital en el interior de la sala. Era muy probable que el SBU, la policía secreta ucraniana, los estuviese vigilando. Y si el SBU estaba al corriente del evento, señal de que también lo estaba el KGB ruso, que por entonces gozaba de plena libertad para ejercer con el SBU una suerte de *droit de seigneur* policial: el derecho a inspeccionar la información en bruto, antes de que su recolector pudiera siquiera examinarla.

A la Familia, el politburó o cúpula de Carder Planet, no le preocupaban demasiado las agencias de inteligencia norteamericanas y europeas ni las operaciones policiales. Pero el KGB era distinto, y no era ninguna coincidencia que la resolución más importante del congreso fuera un aviso contra la ejecución de actividades hostiles en Rusia y Ucrania. «Reiteramos que consideramos inadmisible toda acción dirigida contra nuestros sistemas de facturación, bancos o instituciones financieras», se sentenciaba en ella. Si algún ciberdelincuente rusófono ponía en su punto de mira bancos o negocios rusos, el proyecto entero se iría al traste en menos de cinco minutos.

Pero Carder Planet aguantó bastante más. La web se mantuvo en línea durante cuatro años. Y no resulta exagerado afirmar que sus creadores fueron los responsables del surgimiento y de la consolidación de un método radicalmente nuevo para consumar actos delictivos de grandes dimensiones: fraudes a gran escala reduciendo al mínimo tanto los recursos como los riesgos.

Carder Planet (como sus muchas sucesoras) era ante todo un bazar para vender datos robados —números y códigos PIN de tarjetas de crédito, cuentas corrientes con sus correspondientes contraseñas— y otros productos, como virus y documentación falsa. Hasta entonces, el intercambio de ese tipo de información se producía mediante laboriosas transacciones por ICQ e IRC (los dos sistemas de mensajería preferidos por los *hackers*).

Quienes se dedicaban a la delincuencia informática —tarjeteros, *spammers*, clonadores de tarjetas y creadores de virus— parecían ya una raza aparte de los criminales vinculados a las estructuras mafiosas tradicionales.

Script los llama «lobos solitarios» en una entrevista aparecida en *Hacker* (Xaker.ru), la gran cronista del submundo cibernético ruso: «No se organizan en grupos ni forman sus propias redes; cada cual trabaja por su cuenta y para sí mismo».

Los rusos no fueron los únicos *hackers* que desarrollaron las técnicas de la delincuencia informática, pero Carder Planet les brindó una estructura —cosa hasta entonces insólita— capaz de aglutinar a todos esos lobos solitarios en jaurías provisionales para perpetrar delitos (o simples gamberradas) y, acto seguido, volatilizarse en medio de un inhóspito desierto de bits, camuflados por el bullicio de la red y a salvo de cualquier intento de identificación.

Muy pronto, los miembros de Carder Planet se convirtieron en sus defensores incondicionales: «Hay que entender —dijo uno de los antiguos consejeros pertenecientes al núcleo duro de la página— que Carder Planet no era solo una fuente de información. Vivíamos en ella; la llamábamos el Planeta, como si fuera nuestra casa».

El robo, el *spam* y demás fechorías electrónicas representaban una parte importante de su actividad, pero no eran ni mucho menos el único motivo por el que los *hackers* rusos desembarcaban en el Planeta y establecían ahí su morada. El usuario tipo era un individuo fascinado por la electrónica, la informática, los juegos y las redes, aficionado a infiltrarse en equipos ajenos por pura diversión.

No eran vulgares malhechores que hubieran visto en Carder Planet un nuevo modo de hacer negocio, sino una comunidad de jóvenes, muchos de ellos en torno a los veinte años, decididos a abrirse camino en un contexto histórico caótico y azaroso gracias a sus peculiares conocimientos. En Odesa, quien más quien menos se dedicaba a alguna actividad ilícita, pero la mayoría de la gente se limitaba a actuar en su entorno más directo. Los planetarios, sin embargo, se armaron con la mentalidad de supervivientes típica de la Odesa de aquellos años de agitación política y económica, y replicaron esos patrones de conducta en el ciberespacio. No eran asesinos natos, sino supervivientes natos.

La nueva página se dividía en varias categorías, cada una dedicada a un aspecto concreto de la delincuencia telemática. La primera vez que uno de los jóvenes *hackers* de Odesa se conectó a Carder Planet, se sintió abrumado: «Juro que tuve la misma sensación que debió de sentir Alí Babá al abrir la cueva y encontrarla llena de tesoros. En todas las secciones había montones de información que uno podía usar para hacerse asquerosamente rico ¡sin levantarse de delante del ordenador!».

Durante el primer año, cientos y cientos de *hackers* rusófonos se dedicaron a explorar el sitio, seducidos por sus atractivos gráficos y su eficaz organización. El logotipo de Carder Planet mostraba un hombre elegantemente vestido al que le centellea un ojo mientras fuma un cigarro; parece un doble de Flash Harry, el pícaro al que interpreta George Cole en *The Belles of St. Trinian's*, una de las comedias clásicas de la Gran Bretaña de posguerra.

«Para los muchachos de provincias inocentes como yo, que como mucho podíamos aspirar a ganar cien dólares al mes —continuaba el joven *hacker* de Odesa—, la promesa económica de ese lenguaje desconocido (*dumps, drops, wires, COBs*) era irresistible».

La web no estaba abierta a todos los públicos. Para acceder a las zonas restringidas había que hacerse miembro, y para eso había que superar la criba de los administradores. Aparte de Script, durante el primer año de actividad de Carder Planet otros cuatro miembros asumieron ese privilegiado papel, entre ellos Boa, la mano derecha de Script.

Entre otras cosas, el trabajo de los administradores consistía en decidir a quién aceptar como nuevo miembro y a quién no. En primera instancia, medidas de seguridad como esa estaban concebidas para desviar la atención de las fuerzas del orden y las agencias de inteligencia. El Servicio Secreto estadounidense y el MI6 británico conocían muy bien a los predecesores de Carder Planet, Carder.org y Carder.ru, pero Script estaba decidido a mantenerlos a raya. Confiaba en que la policía local ucraniana no supondría una gran amenaza para la página. «No tienen nada, ni personal ni recursos —afirmaba—. En las agencias ucranianas nadie domina el inglés; en la mayoría de los casos, ni siquiera entienden una palabra. Así que, aunque consigan información sobre el "enemigo", es decir, sobre nosotros, no podrán leerla (ya que tampoco tienen fondos para hacerlo). Resumiendo, no pueden hacer nada».

Pero había un cuerpo más eficaz que la policía ucraniana: sus compañeros rusos del Departamento R del Ministerio del Interior, más tarde reconvertido en Departamento K, especializado en delitos tecnológicos. La policía secreta rusa se infiltró en Carder Planet casi desde su fundación. Pero, tal como señaló el tarjetero bielorruso Police Dog: «A menos que armásemos jaleo a las puertas de nuestra propia casa, la policía local y los servicios de inteligencia no nos buscarían problemas». ¿Por qué iba a emplear recursos el KGB en investigar una red dedicada a estafar con tarjetas de crédito estadounidenses y europeas? Habría sido una monumental pérdida de tiempo.

Por el momento, a Moscú le bastaba con observar y almacenar información. Sabían perfectamente quién era quién en la comunidad tarjetera de Odesa.

Si se considera que Carder Planet y los delincuentes informáticos presentaban un perfil social, cultural y psicológico muy distinto del de los sindicatos criminales tradicionales, no deja de ser irónico que Script y sus colaboradores optasen por designar su estructura organizativa tomando prestada la terminología de la mafia siciliana. *A posteriori*, los tarjeteros reconocerían que el recurso a una metáfora criminal tan obvia fue una equivocación. En su momento, la elección de ese tipo de lenguaje fue un reflejo del perfil psicológico de Script, así como de sus futuras ambiciones como líder de un poderoso movimiento social.

Los miembros más destacados (nunca más de seis) pertenecían a «la Familia», cuyos máximos representantes o administradores tenían derecho al título honorífico de «Padrino». Una vez que esos jefes de la Familia permitían el ingreso de un aspirante en Carder Planet, el nuevo miembro podía explorar las distintas secciones de la web. En una de ellas, por ejemplo, se había colgado una nutrida lista de virus en venta, que podían utilizarse para atacar a otros usuarios. Los creadores de virus también se ofrecían para diseñar *malware* a medida, previo pago, destinado a penetrar en sistemas o programas específicos.

La mayor parte de la actividad se desarrollaba en torno al foro de tarjeteros. En ese apartado se compraban y vendían tarjetas de crédito robadas y datos relativos a cuentas corrientes. «En el curso de su carrera —explica Script—, un tarjetero puede especializarse en una o varias áreas del negocio, pero no hay nadie que domine todas las ramas. Tarde o temprano, el tarjetero necesita de los servicios de alguien. Por eso se ha creado un espacio para redes y grupos; ahí se intercambian números e información. Pueden ser cuentas bancarias, los datos completos de los propietarios de las tarjetas, a veces incluso con el número de pasaporte. También hay tarjeteros que son *hackers* a tiempo parcial, ya que a veces es imposible conseguir la información necesaria (sin pagar) a menos que uno se infiltre en un servidor».

En otro apartado podían adquirirse pasaportes occidentales o permisos de conducción estadounidenses. En la mayor parte de los casos, los documentos falsificados eran de una calidad excelente. Pero ¿cómo podía un comprador estar seguro de ello? Y además: ¿cómo saber que el vendedor no iba a estafarlo? Después de todo, ¡sabía que estaba tratando con un delincuente! Los *rippers* —literalmente «destripadores», delincuentes que estafan a otros delincuentes— ya eran por entonces una presencia habitual en internet.

Esa era la gran baza de Carder Planet. Los miembros de la Familia supervisaban todas las operaciones. Aparte de las cribas, reforzaron la seguridad convirtiendo la página en una web de pago para ahuyentar a posibles alborotadores. Al principio hubo «una gran afluencia de aficionados que saturaron el foro», y Script quiso sacudírselos de encima. Peor aún era la presencia de *rippers*, «que ofrecían servicios de mala calidad o que directamente no prestaban los servicios por los cuales habían cobrado».

Pero Carder Planet no era solo una gran superficie para ciberladrones, ya que el sistema de cribas permitía a los administradores actuar como garantes de los negocios canalizados a través de su web. A cambio, obtenían elogios, dinero y un mercado mucho mayor y más eficaz para sus propios productos.

Script era un *hacker* atípico, en el sentido de que su principal motivación era ganar dinero. Pese a su juventud, fantaseaba con los mares de abundancia en los que nadaba Occidente, sobre todo Estados Unidos. La ambición puede ser, sin duda, un poderoso acicate, pero el genio creativo de Carder Planet no era Script, sino Boa, su estrecho colaborador, para quien el dinero era una preocupación de segundo orden.

El temperamento de Boa era muy distinto del de los demás habitantes del Planeta. Tenía casi cuarenta años cuando Script creó la web, es decir que superaba en dos décadas la edad de la mayoría de sus compañeros y poseía mucha más experiencia que ellos en los negocios de la vida.

En la década de 1980, todavía en tiempos de la Unión Soviética, Boa había dado pruebas de su talento como estudiante de electrónica obteniendo dos títulos universitarios. Sus intereses principales giraban en torno al mundo de las radios de onda corta. Por aquel entonces era una afición delicada, ya que la inteligencia soviética (y, en el caso de las radios de onda corta, la inteligencia militar) se empeñaba en controlar todas las comunicaciones entrantes y salientes del país.

Boa gozaba de gran popularidad gracias a su carácter afable, a veces carismático. Aunque algunos de sus amigos daban por hecho que trabajaba para la sección de comunicaciones de los servicios de inteligencia militar, se convirtió en un icono entre la comunidad de radioaficionados de todo el mundo, que, como es fácil imaginar, reúne a un elevado porcentaje de personajes retraídos y más bien raros.

Boa se labró una reputación en todo el mundo al convertirse en el primer radioaficionado que consiguió emitir desde las islas Spratly, zona restringida bajo control militar vietnamita, a lo que siguió un logro si cabe mayor: la transmisión de las primeras señales de radio desde Corea del Norte. Aquel

triunfó le valió que su nombre fuera celebrado desde Europa hasta Australia, y que, a lo largo de la década de 1990, los fans acudieran en tropel a las convenciones en las que hacía acto de presencia. Gracias a su expresividad y talante, la gente caía a sus pies al momento y todo el mundo quería ser su amigo.

Boa descubrió Carder Planet navegando por la red en el otoño de 1999 y enseguida quedó fascinado por el espíritu emprendedor, aunque caótico, de la página. Por entonces residía en Malta, donde dirigía un próspero negocio de venta de aparatos de vigilancia y contravigilancia a políticos y hombres de empresa de más de sesenta países de todo el mundo.

Conocedor de la experiencia profesional de Boa y de sus capacidades organizativas, Script lo invitó a unirse a la Familia al cabo de unos meses. Impresionado por el brío y la energía de Script, Boa aceptó entrar a formar parte de Carder Planet a principios de 2002. «Cuando Boa se unió al equipo, le insufló nueva vida al Planeta —recuerda uno de los jóvenes habitantes del Planeta—. Él fue el responsable de la sencillez de su diseño e introdujo varias secciones nuevas. Se convirtió en una celebridad en el mundillo».

Al mismo tiempo, Boa acordó con Script la creación de una segunda página web, Boa Factory, que actuaría como complemento de Carder Planet e impulsaría otras ramas del negocio: Boa Factory sería conocida, entre otras cosas, como proveedora especializada en pasaportes y documentos de identificación falsos, así como en la venta al por mayor de tarjetas de crédito clonadas y *dumps*. Mientras que Boa era un sitio web exclusivamente profesional, Carder Planet fomentaba la vertiente social de la clandestinidad, ofreciendo un lugar donde encontrarse, charlar, comprar y vender en la red.

Boa Factory introdujo una herramienta revolucionaria, más tarde adoptada por Carder Planet, que permitió el aumento de la delincuencia informática a escala industrial. Para los ciberladrones el mayor inconveniente residía en la certeza de que las personas con quienes trataban también eran delincuentes y, por ello, gente de poco fiar. Boa concibió un sistema de fideicomiso, conocido en un principio como «servicio de garantía», para resolver el problema. El vendedor suministraba al fiduciario una muestra de su mercancía (por ejemplo, una docena de números de tarjetas de crédito con sus números PIN) y, al mismo tiempo, el potencial comprador le remitía el dinero. El fiduciario probaba la mercancía y, si reportaba las ganancias prometidas, daba vía libre para que el dinero llegase al vendedor y los *dumps* y números PIN al comprador. La genialidad del plan estribaba en su sencillez.

Con él, el negocio quedaba protegido y, a partir de entonces, su éxito no hizo sino aumentar.

Fue Boa quien tuvo la idea de reunir a la Familia en el Primer Congreso Mundial de Tarjeteros en el verano de 2002. Su invitación tendía un puente electrónico entre los distintos puntos de la antigua Unión Soviética, y los destinatarios estaban más que dispuestos a costearse el vuelo (aunque seguramente lo cargaran a tarjetas ajenas). ¿Rechazaría un católico la ocasión de visitar Lourdes? ¿O un musulmán la oportunidad de ir a La Meca? Del mismo modo, ningún delincuente de prez habría dejado pasar la oferta de pasar una semana en Odesa.

El Planeta vivía un momento dulce. Sus usuarios se deshacían en elogios hacia las oportunidades de enriquecimiento que ofrecía, y cientos de *hackers, crackers* y *spammers* esperaban nerviosos a que la cúpula les concediera el valioso privilegio de aceptarlos como miembros.

Script preparó el terreno para la reunión concediendo la primera entrevista pública de un tarjetero profesional. Xaker.ru (la web de la revista *Hacker*), que en la actualidad sigue publicándose, es la biblia de la clandestinidad rusa, pero hasta sus lectores se quedaron estupefactos al leer cómo Script revelaba los secretos del Planeta en marzo de 2002: «¿Por qué uno se convierte en tarjetero?», le preguntaba la revista a Script, señalando que el famoso Departamento R había sido creado para cazar a tarjeteros y similares.

> *Script*: Porque se lo dictan la cabeza y el corazón. La ciencia ha demostrado que quienes se enfrentan al riesgo experimentan un incremento de la llamada hormona de la felicidad. Esa hormona, multiplicada por el murmullo de una cantidad cualquiera de dólares, resulta decisiva a la hora de motivar a alguien para que siga trabajando en esta industria, no del todo honrada.
>
> *Hacker*: ¿No sienten remordimientos?
>
> *Script*: Ninguno. No solo porque cualquiera puede cancelar un pago, aunque haya transcurrido mucho tiempo, con solo enviar al banco una declaración a tal efecto, sino también porque el tarjeteo no es un oficio tan ruin como pudiera parecer. Es mucho menos reprobable que robar con violencia. A los dueños de las tarjetas no les causamos ningún trastorno; si lo piden, el banco se lo devuelve todo, hasta el último penique. Es el gobierno el que debería tener remordimientos por el hecho de

> que los adolescentes se conviertan en desfalcadores a tan corta edad.

Como la mayoría de los tarjeteros, Golubov racionalizaba su negocio: los bancos corren siempre con los gastos, de modo que el ciudadano de a pie no se ve afectado. La simpleza, el sentimentalismo y la demagogia de ese razonamiento pasan convenientemente por alto la manera en que los bancos desvían hacia sus clientes el coste del fraude; en realidad, los tarjeteros tienen un efecto negativo directo sobre las personas corrientes por las que Script mostraba preocupación aparente.

No obstante, su comentario acerca del desinterés del gobierno por el elevado número de jóvenes relacionados con la delincuencia se acerca más al blanco. Ucrania era poco menos que un Estado mafioso y el ejemplo que daban sus dirigentes políticos y hombres de negocios era pésimo. Script se limitaba a seguir ese modelo.

En un contexto como ese, era lógico que Script creyera que con Carder Planet podría reunir el capital necesario para ingresar en la liga de los grandes hombres de negocios del país. Su ambición no conocía límites.

¿Qué podía salir mal?

7

BOA CONSTREÑIDA

Al mismo tiempo que Script lanzaba Carder Planet en Odesa, los investigadores del gigante informático Autodesk decidían en San Rafael, California, que había llegado el momento de ponerse en contacto con el FBI. Autodesk, el mayor productor mundial de programas de diseño en dos y tres dimensiones, vende sus productos por todo el mundo a arquitectos, diseñadores, planificadores urbanísticos, maquetistas, mediadores hipotecarios y fabricantes de vehículos. Además, era el proveedor informático de Grimley Smith Associates, la firma de ingeniería química de Scunthorpe.

Programas especializados como los de Autodesk cuestan su dinero. Los precios de las licencias individuales para los programas de CAD profesionales de Autodesk oscilan entre los tres mil y los siete mil dólares, lo que da una idea de las grandes sumas que la empresa invierte en la investigación y el desarrollo de sus productos.

En 2002, la unidad de protección antipiratería de la compañía descubrió que un vendedor de Ucrania anunciaba en eBay la nueva versión de uno de los programas de diseño de Autodesk por solo doscientos dólares, cuando el precio de venta al público era de tres mil quinientos. «Hmm —debieron de pensar—. ¡Aquí hay gato encerrado!».

Silicon Valley sufre el mismo mal que los estudios de Hollywood. Muchos rodajes requieren inversiones equiparables a las que se necesitan para desarrollar los programas informáticos más complejos. Al mismo tiempo que aumentan los costes de producción, la aparición de los fabricantes de DVD falsos, a menudo vinculados con organizaciones criminales, provoca una bajada en los ingresos. Esto ocurre sobre todo en contextos de recesión: entre desembolsar quince dólares por ver una película en el cine o pagar un dólar por verla en un DVD de impecable calidad dos meses antes de su estreno en las salas, la decisión está clara.

Imaginémonos ahora al propietario de una empresa de un sector competitivo en el que se trabaja, pongamos por ejemplo, con un producto de Autodesk. La adquisición del programa requerido más las licencias puede

ascender a casi veinte mil dólares, pero si se lo compra al tipo de Ucrania a través de eBay el desembolso total es de ochocientos. Seamos sinceros: será ilegal, ¡pero es tentador!

Desde la década de 1970, con la salida al mercado de los primeros programas informáticos, las empresas que los producen han intentado en vano desarrollar dispositivos anticopia (igual que con los CD y los DVD). En todos los casos, las medidas protectoras han sido burladas a los pocos días por alguno de las decenas de miles de *hackers* y *crackers* de todo el mundo. A lo largo de las tres últimas décadas, en ese terreno se ha librado una de las luchas más quijotescas de la industria tecnológica.

Los *hackers* de Europa del Este han tenido un papel especialmente relevante en la vulneración de los dispositivos de seguridad de los programas. En la década de 1980, antes de la caída del comunismo, la Unión Soviética encomendó a varios de sus aliados (sobre todo Bulgaria y Alemania Oriental) del CAME, el bloque para el fomento del comercio, el desarrollo de un ordenador personal y la creación de una industria dedicada al *software*. Las características definitorias de los ordenadores comunistas eran las mismas que las del resto de los productos del bloque del Este: su aspecto era horrible y se estropeaban continuamente. Los desafíos a que se enfrentaban los primeros ingenieros informáticos de la región eran tan enormes que, para superar los problemas y errores que les salían al paso, desarrollaron un ingenio extraordinario.

Las industrias informáticas establecidas en Europa del Este a lo largo de la década de 1980 fueron incapaces de competir con Silicon Valley en los años noventa, tras la caída del muro de Berlín, por falta de fondos para invertir en investigación o equipos. Sin embargo, las nuevas y poderosas organizaciones criminales, cuya influencia sobre las economías de los antiguos países comunistas era más que perceptible, consideraron que el sector tenía un gran potencial. Lo primero que hicieron fue adquirir las plantas de producción (en general por medios más bien turbios); a continuación, contrataron a aquellos talentosos ingenieros para producir programas pirata a gran escala. Bulgaria, Ucrania y Rusia marcaban el paso, y Rumanía las seguía de cerca.

Se entiende ahora por qué Autodesk, al descubrir que un vendedor ucraniano ofrecía cantidades significativas de sus productos pirateados en Estados Unidos, se vio obligada a actuar. Tras meditarlo, decidieron llamar al FBI, que a su vez alertó a la fiscalía de San José, California. Dado que el fraude involucraba a eBay, la fiscalía recurrió a un investigador en concreto:

Greg Crabb, del Servicio de Inspección Postal estadounidense (USPIS), por aquel entonces con base en San Francisco.

Los cuerpos de seguridad competentes en casos de delito informático son tres: el FBI (pues su deber es combatir el crimen), el Servicio Secreto (porque entre sus funciones se halla velar por la moneda estadounidense y prevenir las estafas con tarjetas de crédito) y el USPIS (cuyo fin es controlar todas aquellas actividades delictivas relacionadas con el servicio federal de correos). Si este último cuerpo se implicó en el caso, fue porque las estafas perpetradas a través de eBay y similares conllevaban a menudo el envío de mercancías por correo (tanto si se trataba de bienes adquiridos de forma ilícita como de operaciones de blanqueo de capitales).

Durante los últimos quince años, el USPIS ha reunido un formidable equipo dedicado a la investigación de delitos tecnológicos. La fama de Greg Crabb llegó a tal extremo que acabó dejando San Francisco para dirigir en Washington la Unidad Global de Ciberinvestigaciones, situada en un enorme y anodino edificio del enorme y anodino complejo conocido como Federal Center (se aconseja al lector que lo tache de la lista de lugares interesantes si alguna vez visita la capital de Estados Unidos).

El aire teutónico de Crabb, así como su áspera forma de arrastrar la voz al hablar, lo hace a la vez temible y atractivo. Se formó como contable, y parece ser de esos a los que uno, aunque tenga las manos limpias, nunca dejaría meter las narices en su declaración de impuestos por miedo a ser hallado en falta. Profesionalmente, para Crabb eso supone una gran ventaja, ya que ser capaz de revisar largas listas de cifras, mensajes cortos y datos a primera vista incomprensibles es condición *sine qua non* para ser un buen ciberpolicía. Suena emocionante pero, como todo lo relacionado con la informática, la mayor parte del tiempo es de un aburrimiento mortal.

Una vez destinado al caso de Autodesk, Crabb rastreó adónde enviaban el dinero los compradores de los programas pirata. Resultó que los pagos iban a parar a una serie de cuentas corrientes pertenecientes a quince «mulas», ciudadanos estadounidenses repartidos por todo el país. Las estafas y el blanqueo de capitales dependen de estos colaboradores (en su mayoría) involuntarios, gente que contesta a anuncios que prometen suculentas ganancias a cambio de trabajar desde el ordenador de casa. A los candidatos admitidos se les pide que pongan sus cuentas corrientes a disposición de su nuevo jefe. En el caso de Autodesk, las mulas recibían doscientos dólares la primera vez y, en lo sucesivo, ciento ochenta, pues se quedaban veinte en concepto de comisión. Su trabajo consistía en transferir el dinero a un banco

de Letonia, uno de los tres Estados bálticos cuya contribución a la delincuencia telemática, y al problema de la inseguridad informática en general, resulta desproporcionada si se compara con los siete millones de habitantes que cuenta en total.

Con la ayuda de la policía letona, Crabb averiguó que el destino último del dinero eran una serie de bancos de Ternopil, en el oeste de Ucrania. Todas las cuentas pertenecían a un tal Maksim Kovalchuk o a su esposa.

Crabb se daba cuenta de que Kovalchuk no suponía ningún riesgo para la economía estadounidense. En comparación con las cifras que mueve normalmente el crimen organizado, la cantidad que Kovalchuk ingresaba con su estafa era irrisoria, aunque para Autodesk resultara sangrante. Crabb intentó acceder a la cuenta de correo de Kovalchuk para descubrir si contenía más secretos. Durante el proceso encontró «la manera» de controlar sus comunicaciones, lo que debe interpretarse, o bien como que logró infiltrarse en su ordenador, o bien como que convenció a su proveedor de correo para que le permitiese acceder a él. Sea como fuere, el éxito de Crabb tuvo consecuencias decisivas, ya que al leer sus correos averiguó que Kovalchuk estaba implicado en un proyecto mucho más ambicioso que la estafa de Autodesk: el desarrollo de una web llamada Carder Planet.

Aunque el objetivo principal seguía siendo Kovalchuk y su relación con la estafa, Crabb empezó a reseguir las ramificaciones de Carder Planet como segunda línea de investigación. Ignorante de que Estados Unidos le seguía la pista, Kovalchuk no tomaba muchas precauciones a la hora de comunicarse, así que, gracias en parte a la suerte y en parte a su concienzuda labor, Crabb se hallaba en una posición ventajosa. No solo podía prever los movimientos de Kovalchuk, sino que hasta les había tomado la delantera a las agencias de inteligencia occidentales. Al penetrar en la comunidad de ciberdelincuentes más dinámica del mundo, Crabb había triunfado donde hasta entonces los cuerpos occidentales habían fracasado.

El problema era que, por mucho que Crabb averiguase sobre la comunidad *hacker* de Ucrania, no podía hacer gran cosa. Ni siquiera podía detener a Kovalchuk. No solo no existía convenio de extradición entre Estados Unidos y Ucrania, sino que la tesitura política de ese gran país del este de Europa era de lo más delicada. Leonid Kuchma presidía por entonces el país, entrecruzado por una amplia red de relaciones corruptas entre oligarcas y mafiosos. Estados Unidos, además, se hallaba en disputa con Europa y Rusia por ejercer su influencia en Ucrania, pero en esos momentos

los vientos dominantes soplaban con fuerza desde Moscú. Mientras no saliera de Ucrania, Kovalchuk podía considerarse a salvo.

A todo esto, a finales de 2002, mientras el inspector Crabb estaba todavía en San Francisco, se puso en contacto con él el departamento de seguridad de Visa, cuyo cuartel general se halla en la misma ciudad. La dirección estaba desesperada por culpa de un *hacker* llamado Boa que había robado, o ayudado a otros a robar, decenas de miles de tarjetas de crédito a través de su famosa web, Boa Factory. Crabb dio un respingo: el nombre de Boa le sonaba de varias conversaciones leídas en la cuenta de Kovalchuk. Si mal no recordaba, Kovalchuk había realizado multitud de compras en Boa Factory, donde había aprendido los trucos del oficio y había participado en las discusiones acerca del desarrollo de Carder Planet. Poco después, el inspector identificó a Boa y Script como las figuras centrales de Carder Planet. Con discreción, mandó una nota a través de Interpol por la que instaba a las demás fuerzas del orden a contactar con él en caso de detención de ciudadanos ucranianos sospechosos de delitos tecnológicos.

A finales de febrero de 2003, Roman Vega regresaba de un viaje de negocios a su casa de Malta cuando uno de sus amigos le pidió que fuera a visitarlo a Nicosia, Chipre. Pasaron la noche bebiendo y recordando sus aventuras en Birmania, donde, en 1991, habían formado parte del equipo de aficionados que realizó la primera emisión de radio del país, entonces bajo régimen militar.

Al volver a su habitación del hotel Castelli, Vega se encontró con una desagradable sorpresa: Modesto Poyiadjis, inspector de la policía local, procedió a arrestarlo por complicidad en un caso de fraude de tarjetas de crédito perpetrado por otro ciudadano ucraniano al que Vega había permitido alojarse en su habitación (decisión, según se ve, equivocada). Para Vega, fue el principio de una relación con las fuerzas de la ley chipriotas y estadounidenses que solo cabe calificar de kafkiana.

Tras revisar los archivos de Interpol, Poyiadjis se puso en contacto con Greg Crabb, el agente a cargo de la investigación de Boa en Estados Unidos. El inspector le informó a Crabb que estaba convencido de que Roman Vega no era otro que Boa. Crabb no cabía en sí de emoción. Antes de colgar el teléfono, ya estaba reservando billete para el primer vuelo con destino a Nicosia. No se trataba tan solo de intentar extraditar a uno de los cerebros de Carder Planet, sino que, además, ¡tenían su ordenador! Si los chipriotas habían conseguido identificar a ese tipo con su *alter ego* sin saber muy bien

qué se traían entre manos, qué no podría descubrir un investigador como Crabb en su disco duro.

«La detención de Boa fue un duro golpe», asegura Xhora, miembro de Carder Planet, haciéndose eco del sentir de muchos de sus cibercompatriotas en ese momento. Gracias a Boa, Carder Planet se había convertido en una página divertida, interesante y lucrativa. Por ser mayor y más experimentado que el resto de los habitantes del Planeta, muchos lo creían inmune a peligros como las fuerzas de la ley.

Mientras esto sucedía, Script acaparaba cada vez más poder y dinero de resultas de su posición en Carder Planet. «Sus entrevistas tenían como fin incrementar la popularidad de la página y aumentar el volumen de negocio —asegura Null_ Name, otro de los habituales de Carder Planet—, y hay que decir que lo consiguió. La afluencia de nuevos miembros era continua. Pero el ambiente cambió. Dejó de ser lo que era».

La cordial camaradería de los primeros días, en efecto, iba desapareciendo a gran velocidad, pero aun así las ganancias de la web eran mayores que nunca. Se añadió una sección en inglés en el foro, y, al poco tiempo, tarjeteros del mundo entero empezaron a darse de alta en la página. Entretanto, muy lejos, en San Francisco, Greg Crabb se daba un verdadero festín con el disco duro de Boa, de donde extrajo los mil y un secretos que Boa y Script tenían entre manos. «Nunca tuve que entrevistarme con Boa —afirma Crabb—. Ni siquiera me interesaba lo que tuviera que decir, porque estaba todo en su disco duro. No podía añadir nada nuevo».

Sin embargo, es posible que Crabb no pudiera registrar el ordenador todo lo bien que habría querido. Por lo visto, los investigadores estadounidenses rompieron el sistema de encriptación del VAIO de Boa, pero este lo había reforzado con otro potente programa llamado Handy Bits EasyCrypto (de descarga gratuita), que habría impedido el acceso al ochenta por ciento de los archivos del equipo.

En los foros de tarjeteros aún hoy se perciben signos de descontento, ya que sus miembros dan por seguro que Roman Vega delató a Golubov. Mentira: todo lo que se averiguó sobre Golubov procedía de los datos almacenados en el VAIO. Vega no solo guardó silencio, lo cual tuvo para él un coste personal considerable, sino que se ha pasado casi diez años en varias prisiones chipriotas y estadounidenses sin haber sido condenado por ningún delito en concreto.

A pesar de la nueva información, Crabb todavía no podía hacer nada contra Script, que no salía de Ucrania, a diferencia de Maksim Kovalchuk,

que fue arrestado junto con su mujer por la estafa de Autodesk en una lechería de Bangkok tres meses después de la detención de Roman Vega en Nicosia. Al igual que Vega, que desde Chipre fue extraditado a California, Kovalchuk salió de Tailandia con destino a la Costa Oeste de Estados Unidos.

Script no solo no tenía ninguna intención de abandonar su país natal, sino que, para blindarse aún más, a principios de 2004 anunció en Carder Planet que dimitía de su cargo en la dirección y se desvinculaba de la página.

Script, como siempre, tenía un plan. Las tarjetas —cuyo robo, como se ha visto, no le causaba remordimientos— le habían reportado un dinero que podía invertir en negocios legítimos. Quizá lo hiciera por evitar sorpresas desagradables en el futuro, o tal vez porque tenía ambiciones más allá del ciberespacio. En cualquier caso el anuncio no dejaba lugar a dudas: cedía las riendas de la página a uno de sus *consiglieri* de confianza y abandonaba para siempre la órbita del Planeta.

Por lo visto, Script había hecho propósito de enmienda. Entonces ocurrió algo con lo que no había contado.

La revolución.

8

SCRIPT BORRADO

Boris Borisovich Popov llamó a la oficina para avisar de que se encontraba indispuesto. El médico, explicó, le había aconsejado unos días de reposo. Algunos de sus colegas se mostraron sorprendidos. La menuda complexión y los rasgos adolescentes de Boris Borisovich recordaban en ocasiones a los de un niño enfermizo, pero en realidad era uno de los trabajadores más aplicados y disciplinados de la plantilla. «Daba gusto trabajar con él —diría más tarde uno de ellos—, no había nadie mejor en todo el servicio».

En lugar de guardar cama, Popov —que de hecho rebosaba salud— salió de su apartamento, paró un taxi y se dirigió al aeropuerto Borispol de Kiev, donde embarcó en un vuelo para Odesa. Originario de Donetsk, en el este de Ucrania, y con el ruso por lengua materna, su presencia en el sur no levantaría sospechas, siempre y cuando se anduviera con cuidado.

Nada más llegar a Odesa, tomó el autobús que llevaba a la ciudad. Era un caluroso día de julio. La temperatura bordeaba los treinta grados, pero la alegre brisa del mar Negro la hacía soportable. Popov no tardó en encontrar el apartamento que había alquilado. Pocas horas después, llegaron sus tres compañeros de equipo: Natasha Obrizan y los señores Grishko y Baranets. «No podíamos alojarnos en un hotel —explica Boris— porque desconfiábamos de la policía local». Solo otra persona en todo el país sabía que se encontraban en Odesa: el ministro del Interior.

Seis meses antes, el país había sufrido una virulenta convulsión: la revolución naranja. Ucrania es un país excepcionalmente fértil, con potencial para suministrar por sí solo alimento a casi toda Europa, pero ello no le ha ahorrado tragedias. A lo largo del siglo XX conoció el nacionalismo extremo, la autocracia, el comunismo y el fascismo; cada cual a su manera, todos los regímenes se cebaron con la población del país: guerras civiles, hambrunas, genocidios, deportaciones y pobreza generalizada.

El producto más duradero de esta historia de caos ha sido la división de Ucrania en dos regiones geográficas y lingüísticas: la occidental y la oriental;

la ucraniana y la rusa. Kiev, la capital, se halla en medio de ambas a modo de frágil puente, en un intento de conciliar dos tradiciones en ocasiones hostiles. En los días más negros del siglo XX, fueron muchos quienes vieron en la región occidental un símbolo de Alemania y el fascismo, y en la oriental, un baluarte del comunismo moscovita.

No siempre la división es tan clara: en el este pueden encontrarse bolsas de hablantes ucranianos y, a menudo, los candidatos prorrusos cosechan votos inesperados en ciertas zonas orientales. De todos modos, vale como regla general. Desde la independencia, Kiev y las provincias occidentales han luchado por estrechar lazos con la Unión Europea y la OTAN, mientras que la zona oriental ha intentado reforzar sus vínculos con Rusia. De hecho, muchos ucranianos del este todavía se sienten parte del gigante vecino.

Hasta 2004, los distintos gobiernos y presidentes ucranianos habían apoyado la línea prorrusa, para alegría del este y disgusto de los nacionalistas del oeste. Por consiguiente, las relaciones con la Unión Europea, la OTAN y Estados Unidos eran más bien frías: los representantes del gobierno ucraniano pasaban casi tanto tiempo en la Casa Blanca como en las cárceles estadounidenses por blanqueo de dinero y demás actividades propias de la mafia globalizada.

A la vista de que funcionarios, políticos y oligarcas se llenaban los bolsillos a expensas del ciudadano común, cuyo nivel de vida cayó en picado antes y después del cambio de milenio, empezó a fraguarse un nuevo movimiento que gravitaba en torno a dos políticos con un estilo distinto, Víctor Yúshchenko y Yulia Timoshenko. Solo más tarde se supo que estaban cortados por el mismo patrón que sus oponentes. Yúshchenko saltó a los titulares en septiembre de 2004 tras ser envenenado con dioxinas (casi seguro por el KGB). Su rostro quedó gravemente desfigurado, pero sobrevivió al intento de asesinato y anunció que no se retiraría de la carrera por la presidencia.

La campaña para derrocar a la vieja guardia cautivó la imaginación de los jóvenes ucranianos, que la convirtieron en un festival político, conocido como la revolución naranja. Estudiantes y activistas serbios que habían contribuido a deponer a su propio dictador, Slobodan Milošević, llegaban a Kiev para enseñar a sus cuasivecinos cómo sacar partido de aquel fervor político. Estados Unidos, por su parte, presintiendo que aquella era la gran ocasión para darle en todos los morros a Moscú y arrastrar a Ucrania hacia la órbita de la OTAN, envió a sus proselitistas neoconservadores al país.

Aquella repentina oleada de actividad política tuvo consecuencias en la esfera internacional desde el principio. Cuando Yúshchenko fue nombrado por fin presidente y Timoshenko primera ministra, en enero de 2005, Ucrania ya se había convertido en un banco de pruebas viviente de las cada vez más deterioradas relaciones entre Rusia y Estados Unidos. Los dos nuevos líderes no solo se comprometieron a ingresar en la Unión Europea, sino que anunciaron su deseo de que el país en breve pasara a engrosar la lista de miembros de la OTAN. Aunque la iniciativa estaba destinada al fracaso (al fin y al cabo contaban tan solo con el apoyo del treinta por ciento de los votantes ucranianos), Moscú interpretó la acción poco menos que como una declaración de guerra.

En los cuatro años transcurridos desde su primer encuentro con Maksim Kovalchuk —el vendedor de falsos productos Autodesk—, el inspector Greg Crabb había dedicado su paciencia a afianzar las relaciones con colegas de los numerosos cuerpos de seguridad ucranianos. Sin embargo, y pese a contar con contactos importantes, sus solicitudes de arresto contra Dimitri Golubov, alias Script, fueron siempre educadamente rechazadas.

Los decisivos sucesos de diciembre de 2004 y enero de 2005, los meses en que Yúshchenko y Timoshenko alcanzaron el poder, dieron un vuelco a la situación. Crabb entendió que la revolución naranja representaba una oportunidad que no podía desaprovechar. Poco después de aquellos tumultuosos acontecimientos, lo llamaron de la embajada de Estados Unidos en Kiev y le informaron que el Ministerio del Interior ucraniano acababa de depurar al anterior núcleo duro y había reunido un nuevo equipo más dispuesto a colaborar con Occidente. «¡Venga ahora mismo!», le dijeron en la embajada. No hizo falta decírselo dos veces.

El inspector aterrizó en Kiev en junio de 2005 y presentó sus pruebas del caso Golubov ante los funcionarios del Ministerio del Interior. Dos semanas después, el inspector Popov, del Departamento contra el Crimen Organizado, se dirigía a Odesa con instrucciones de localizar y detener al escurridizo Script.

Popov sabía que no iba a ser fácil. Lo que más lo preocupaba eran las filtraciones, ya que, si la noticia llegaba a Odesa antes que él, la operación fracasaría antes de haber empezado. Por lo demás, era probable que Golubov, tarjetero consumado y multimillonario, se hubiera procurado la protección de las fuerzas de seguridad locales. Entre los suyos, era invencible.

La calle Dovzhenko queda tres kilómetros al sur del centro de Odesa. La zona, con sus calles flanqueadas de árboles, es uno de los barrios de moda de

la ciudad. Golubov vivía en el apartamento de su abuela, de aquí la sorpresa de Popov y su equipo cuando, al presentarse en el lugar, se encontraron con una gruesa puerta de acero bloqueándoles el paso. Tras tomar posiciones, Popov hizo una señal a sus compañeros. «¡Abra, policía!», gritaron mientras aporreaban la puerta, que ni se movía. Al otro lado, silencio. Aguzaron el oído por si percibían algo a través del muro de acero; uno de ellos creyó detectar un rumor. Pero, por más que insistieron, la puerta permaneció sólidamente cerrada.

Mientras Popov barajaba la opción de echar mano de la artillería pesada, sus olfatos detectaron el olor acre del papel quemado. «¡Cielo santo! —pensó—. ¡Está quemando pruebas!». Sin perder un segundo, Popov alertó a los servicios de emergencia y, al instante, un camión de bomberos se puso en camino. Como el calor era cada vez más intenso, los bomberos abrieron un boquete en la pared del apartamento y rociaron con espuma el interior. Cuando ya parecía que el apartamento de la abuela iba a quedar anegado por los productos químicos, Golubov decidió rendirse y por fin abrió la puerta.

La escena era indescriptible. Popov no solo se encontró con los archivos de Golubov en llamas, sino al propio *hacker* introduciendo sus discos duros en un Raskat. Si Golubov se hubiera limitado a borrar los archivos de sus varios ordenadores, cualquiera con rudimentos de informática forense habría podido reconstruirlos sin mayor dificultad. El papel puede quemarse, pero los archivos informáticos no se destruyen tan fácilmente. Sin embargo, el Raskat, artilugio de fabricación rusa, emite unas potentes ondas electromagnéticas capaces de destruir los datos por completo. Golubov había sido pillado con las manos en la masa, y Popov se lo llevó a Kiev, donde ingresó en prisión.

Vega y Golubov ya estaban entre rejas (como otros muchos miembros vitales de la familia Carder Planet). Ambos negaron por activa y por pasiva ser Boa y Script. Ninguno de los dos ha sido condenado todavía por ningún delito. A decir verdad, el primero ha pasado siete años en distintas prisiones norteamericanas sin haber sido sometido a un proceso judicial completo, lo que suscita serias reservas acerca de la eficacia del sistema judicial estadounidense.

Sea como fuere, Carder Planet había sido descabezada. Puede que la web que catalizó las ambiciones de tantos *hackers* y *crackers* haya desaparecido, pero su legado es inmenso: gracias a ella, la delincuencia en la red vivió una revolución.

Por otro lado, la delincuencia informática a gran escala ya se había diseminado más allá de la cuna ucraniana. Durante los dos últimos años de

Carder Planet, sus administradores habían impulsado un foro en lengua inglesa que se desarrolló de forma paralela a los paneles de discusión en ruso. Dicho foro contagió el espíritu de Odesa entre *hackers* y tarjeteros del mundo entero. Dos de sus miembros eran principiantes, pero sentían una gran curiosidad por el nuevo mundo del tarjeteo profesional. Uno de ellos adoptó como avatar la figura de un simpático pirata; el otro, una imagen sacada de una de las películas favoritas de muchos *geeks*: JiLsi y Matrix001 entraban en escena.

PARTE III

9

TIGRE, TIGRE

Colombo, Sri Lanka, 1988

¡Pum! ¡Pum! ¡Pum!

«¡Abran! ¡Abran!»

Cuando un grupo de soldados grita esto, rara vez esperan respuesta, y mucho menos a las cinco y media de la madrugada. Tras abatir la puerta a golpes de fusil, entraron en tropel en la casa. Avanzaron habitación por habitación, ordenaron a los miembros de la familia que se echaran al suelo y revolvieron el domicilio de arriba abajo.

Con el ruido y las luces, los tres jóvenes se despertaron aterrorizados. «¡Fuera de la cama! ¡Fuera de la cama!». Los muchachos, sudados por el calor tropical y sin más vestimenta que la ropa interior, notaron que las mandíbulas les temblaban de miedo. Los soldados separaron al mayor, de solo once años, y señalaron una porción de piel blanca del tamaño de una mano que tenía en el estómago. «¿Qué es esto? ¿Qué es esto? —gritaron con voz casi triunfal—. ¡Ha estado manipulando explosivos!».

«¡Es una mancha de nacimiento! —contestó—. ¡Solo es una mancha de nacimiento!».

Se llevaron al muchacho aparte y, antes de empezar a interrogarlo, lo hicieron sentarse en una de las sillas del salón. Los padres y la abuela le suplicaron al soldado que parecía estar al mando. Al final, los soldados concluyeron que aquel muchacho de figura endeble que todavía no había dado el paso a la adolescencia no tenía aspecto de fabricar bombas para los Tigres Tamiles.

El pequeño Renu estaba acostumbrado a esa clase de sobresaltos. Su vida había estado salpicada por sucesos de ese tipo desde la más tierna edad. Cinco años antes, en julio de 1983, con solo seis años, había sido evacuado de Colombo. Los militantes tamiles habían abatido a trece soldados del ejército de Sri Lanka. En represalia, una muchedumbre de cingaleses había asesinado

a cientos de tamiles inocentes en la capital, Colombo, desencadenando una prolongada guerra civil que no terminaría hasta veintiséis años más tarde.

Esperar sentado a que las bandas cingalesas acabasen de saquear la ciudad era impensable, así que los padres de Renu hicieron las maletas y se llevaron a sus tres hijos a Jaffna, la principal ciudad de la comunidad tamil de Sri Lanka. Situada en el extremo septentrional del país, Jaffna se halla a solo ochenta kilómetros de la costa sudeste de la India. Además, era el bastión de las milicias tamiles. La resistencia contra el gobierno de Colombo, dominado por los cingaleses, era cada vez más fuerte.

Al poco tiempo, la impredecible violencia de la guerra civil y la insurgencia empezó a propagarse hacia el nuevo hogar de Renu. En 1987, las tropas gubernamentales pusieron sitio a Jaffna, donde los infames Tigres Tamiles fueron combatidos por varios grupos armados, en especial los TLET. El flujo de refugiados que abandonaba la ciudad en dirección al sur de la India a través del estrecho de Palk alcanzó dimensiones críticas, ante lo cual el gobierno de Nueva Delhi se vio obligado a actuar. En virtud de un acuerdo con el gobierno de Sri Lanka, la India envió a Jaffna una nutrida fuerza de pacificación con la misión de supervisar un acuerdo de paz.

Las relaciones entre los pacificadores indios y los Tigres Tamiles no tardaron en truncarse y Jaffna volvió a convertirse en una de las ciudades más peligrosas de la Tierra. En octubre de 1987, las tropas indias masacraron a varias docenas de civiles en el principal hospital de la ciudad; en veinticinco años de guerra civil, aquel fue el único suceso que logró unir al gobierno de Colombo y a los Tigres Tamiles. Para Renu y su familia, el riesgo de permanecer en Jaffna era demasiado alto, de modo que decidieron regresar al sur, a Colombo.

Una tarde, el padre de Renu le pidió al muchacho que fuera a comprar comida. Renu, que nunca había visto tantas rupias juntas, se las guardó en el bolsillo junto con la lista de la compra. De camino a la tienda, vio a un hombre que jugaba a un juego al lado de la carretera. Había tres cubiletes y, debajo de uno de ellos, una piedrecita. Renu vio cómo la gente apostaba por uno u otro de los cubiletes después de que el hábil charlatán los hubiera cambiado de sitio a la velocidad del rayo. Renu quedó maravillado y sorprendido al comprobar que los jugadores fallaban invariablemente a la hora de señalar dónde estaba la piedrecita, mientras que él, en cambio, habría acertado todas las veces. Se abrió paso hasta el principio de la fila y sacó los arrugados billetes que le había dado su padre. Al igual que quienes lo habían precedido, Renu erró cubilete y, uno a uno, los billetes fueron pasando al

bolsillo del hombre. Cuanto más perdía, más frenéticas se hacían sus apuestas. Era incapaz de parar. Al final, se le acabaron los billetes y su menudo cuerpo, rebosante de adrenalina, empezó a exudar un sudor frío. Justo entonces, vio a su padre con la mano levantada encima de su cabeza. Nunca volvió a apostar.

En los años transcurridos desde la salida de Jaffna, la capital se había calmado un poco, aunque la seguridad de los tamiles nunca estuvo del todo garantizada, como bien lo demostró el asalto de los soldados a su casa. Pero, para entonces, a la familia de Renu ya casi se le habían acabado las opciones.

Renu, que aún no abandonaba la infancia, se había pasado buena parte de su vida yendo y viniendo del fuego a las brasas, en ocasiones salvándose literalmente por los pelos. Poco después de que los soldados asaltaran su casa y confundieran al chiquillo con un terrorista por culpa de una mancha de nacimiento, la madre de Renu decidió que la situación en la capital de Sri Lanka era demasiado peligrosa para un preadolescente tamil. Podía sentirse tentado de unirse a los Tigres o meterse en problemas con los grupos nacionalistas cingaleses que merodeaban por la ciudad.

En 1992, la familia había reunido el dinero suficiente para enviar a Renu a Londres, donde vivían sus tíos.

Aquella nueva vida, en la otra punta del mundo, en un ambiente totalmente distinto, tenía también sus peligros. En la Langdon School —una de las escuelas más grandes y conflictivas del este de Londres—, Renu, bajito y de constitución endeble, se vio atrapado entre dos grandes comunidades, la blanca y la bengalí. Se le daban bien las matemáticas, en las que aventajaba a todos sus compañeros, pero apenas conseguía expresarse en inglés. Se convirtió en un marginado y padeció acosos continuos. Tanto fue así que, pasados seis meses, se negó a volver a clase, pese a los ruegos de sus desesperados tíos.

El muchacho estuvo dos años encerrado en casa; a veces pasaba semanas sin salir al aire libre. Lo único que hacía era ver televisión día y noche.

Así fue como Renukanth Subramaniam aprendió a soportar la soledad.

Y quizá se habría instalado en ella de forma definitiva de no ser porque su tío lo obligó a volver al mundo exterior, en concreto al Newham College for Further Education. Ahí aprendió nuevas destrezas: a relacionarse con sus compañeros, a fumar marihuana, a beber *brandy* Martell y a programar ordenadores.

En el *pub* local, Renu, aunque estuviese fumado y bebido, machacaba a sus oponentes virtuales de *Street Fighter*. ¿Cuántos jóvenes se vieron atraídos

de forma obsesiva por esa afición hipnotizante y repetitiva, en la que el jugador se enfrentaba, por medio de un avatar, a una serie de batallas a muerte contra una retahíla de agresivos luchadores? ¿Era ese un medio de aplacar la agresividad o de fomentarla? ¿Provocaba la dopamina segregada en el lóbulo frontal del cerebro —que con esos juegos se dispara— una intensa adicción en todos los jóvenes o quizá solo en algunos?

Renu aporreaba la máquina con el cuerpo empapado en adrenalina y el cerebro rebosante de endorfinas. Al terminar, todavía en tensión, se entregaba al Martell para prolongar la sensación de bienestar y relajarse. Poco a poco, sus hábitos empezaron a hacer estragos en su de por sí escasa paga. El *Street Fighter* ocupaba un lugar cada vez más importante en su vida. Cuando se iba a dormir, las violentas imágenes del juego reaparecían en tecnicolor en su imaginación.

De la misma manera que años atrás había dejado de apostar, resolvió no jugar más, y nunca volvió a tocar un videojuego. Por desgracia, la renuncia se limitó únicamente al *Street Fighter* y no a su creciente afición a la bebida y las drogas.

Que hubiera repudiado los videojuegos no significaba que renunciase a su fascinación por los ordenadores. Había tenido su primer contacto con ellos a los nueve años, en Sri Lanka, y desde entonces le encantaban. Como no tenía dinero, no podía acceder a ellos de forma regular. Pero el problema desapareció cuando, con poco más de veinte años, aceptó una plaza para estudiar informática en la Universidad de Westminster, en Londres.

Poco después, Renu descubría los *warez*, programas pirateados cuyos sistemas de seguridad habían sido descifrados y distribuidos entre una serie de iniciados conocidos como la Escena.

En ese mundo podía tener amigos y, a la vez, estar solo.

10

TEORÍA DE JUEGOS

Eislingen, Baden-Württemberg, 2001

Mientras Renu exploraba la Escena, a ochocientos kilómetros, en el sur de Alemania, otro usuario tropezaba con la misma misteriosa comunidad.

Matrix001 tenía quince años y estaba enamorado. Pero no de una chica. A Matrix lo que lo volvía loco eran los videojuegos. Empezaron siendo una más de las actividades a las que un adolescente normal y equilibrado dedica su tiempo libre, junto con la gimnasia y la orquesta de la escuela, en la que tocaba el clarinete. A primera vista, todo era normal. Sabía cómo disimular su secreta obsesión por los videojuegos. Nadie —ni amigos, ni padres, ni hermanos—, a excepción quizá de su hermano pequeño, tenía la menor idea.

No solo le encantaba jugar, sino que se le daba bien. Pero, a medida que se acercaban los exámenes de graduación, sus sesiones frente al teclado empezaron a robarle horas de sueño. Mantenerse al día de las últimas novedades salía caro, sobre todo cuando (como en el grupo de jugadores al que pertenecía Matrix) el prestigio de uno dependía de haber jugado y superado juegos recién aparecidos en el mercado.

En el año 2000, la afluencia de novedades con gráficos nunca vistos era continua. En cuatro días apareció la serie de Pokémon y, al otro extremo del espectro, *WWF Smackdown 2: Know Your Role*, que fue la sensación se la temporada junto con *Grand Theft Auto*, con sus característicos guiones violentos y pornográficos. Matrix se volvía loco por hacerse con los últimos juegos, pero no podía permitírselos todos.

En lo relativo a los juegos, su vida parecía un reflejo de la de Renu. En lo demás, no tenían nada en común.

Decidido a satisfacer su gran pasión, Matrix descubrió una comunidad de internet conocida como escena fXp. El fenómeno se reveló crucial, no solo para la vida de Matrix, sino para los tornadizos parámetros de la cultura de internet.

En las dos décadas transcurridas desde su introducción, el ordenador personal se había convertido en el centro de un apasionado, aunque críptico, debate —entre desarrolladores, vates y usuarios iniciados— a propósito de su papel en la sociedad. Muchas de las actividades delictivas que se consuman en la red tienen su origen en una escisión de base en el debate filosófico generado por la aparición de internet.

Simplificando un poco, el debate bascula, por un lado, entre quienes creen que lo principal es su valor comercial y, por otro, quienes opinan que se trata en última instancia de una herramienta social e intelectual cuya naturaleza altera el código moral fundamental de la comunicación de masas. Para los primeros, copiar «códigos» informáticos (los lenguajes en que los programas reciben instrucciones) sin permiso explícito constituye una infracción. Los segundos, por el contrario, están convencidos de que, a partir del momento en que se ofrece al público un programa, se renuncia a todo derecho de autoría.

El núcleo de la discusión se remonta a febrero de 1976, a una carta abierta enviada por Bill Gates a la incipiente comunidad de usuarios de la que saldrían muchos *geeks*, *hackers* y *crackers*. En ella, Gates lamentaba que el 90 por ciento de los usuarios del primer lenguaje de programación de Microsoft, el Altair BASIC, no lo hubiera comprado, sino que lo hubiera copiado, de modo que Gates no obtenía ganancias por la enorme cantidad de trabajo y dinero invertidos en su desarrollo. Aunque el estilo de Gates acusaba la inelegancia típica de los *geeks*, el mensaje era diáfano: acusaba a los usuarios de robarle.

Los aficionados, *geeks* y *hackers* —o *crackers*, como se los llamaría más tarde— discrepaban. Desde su punto de vista, una vez publicado el «código», todo vale. Desde la Costa Oeste hasta el MIT, en Cambridge, Massachusetts, algunos de los más importantes desarrolladores informáticos, así como algunos usuarios de primera hora, se vieron infectados por una fuerte dosis de ideología «cumbayá» que defendía que la tecnología estaba hecha para unir al mundo y que existían motivos (no concretados) para no someterla a las normas de propiedad intelectual aplicadas tradicionalmente a los libros, la música y otros productos creativos.

La razón era evidente: tiempo atrás, el público era incapaz de imprimir ejemplares sin licencia de un libro o de producir vinilos pirata de un álbum, pues carecía de la maquinaria necesaria para ello. Y si la poseía, se trataba de equipos pesados y fijos, por lo que la policía no tenía problemas en confiscarlos en nombre de la propiedad intelectual.

Los códigos y los programas eran harina de otro costal. Una vez desterradas las cintas de casete que a comienzos de la década de 1980 contenían los primeros juegos de ordenador de uso doméstico, los códigos empezaron a inscribirse en disquetes, CD, DVD y discos duros de tamaño cada vez más reducido. Fue entonces cuando el imperio de los productores de *software* comercial ensayó su primer contraataque insertando partes de código adicional en sus productos con el fin de evitar copias no autorizadas de su material. Muchos CD y cintas de casete llevaban incorporado ese cerrojo digital.

Era un movimiento comprensible, pero acabó volviéndose en su contra. En 1982, otro adolescente alemán, que más tarde adoptaría el enigmático apodo de MiCe!, convenció a sus padres —contra la sensata opinión de estos — de que le comprasen un ordenador por Navidad. Como el desembolso era considerable, se negaron a darle un solo céntimo más para juegos, ignorando que, sin programas —por entonces venían en cintas de casete—, el ordenador no servía para nada.

El muchacho llegó a la conclusión de que solo había una manera de sacar partido al ordenador: haciendo copias de los programas de sus amigos. Hasta que un día dio con una cinta que no se copiaba. Lo probó por todos los medios imaginables, pero el ordenador siempre se acababa colgando. Tras días y noches de frustración, identificó en un punto concreto de la cinta un fragmento de código sin función aparente. De pronto lo vio claro: ¡eso era lo que bloqueaba el proceso! MiCe! empezó a experimentar reescribiendo el código en diferentes secuencias, hasta que una noche —¡bingo!— consiguió romperlo.

Los jugadores de primera hora como MiCe! fueron quienes empezaron a romper los cerrojos, pero no por ganar dinero, sino por su adicción a los juegos. Las copias circulaban de mano en mano, y así nació la Escena.

Por entonces se trataba todavía de un proceso largo y laborioso, pues requería copiar físicamente el código en una nueva cinta. Pero los aficionados a los juegos recogieron encantados el guante arrojado por los productores de *software* y, al poco tiempo, empezó a florecer una importante subcultura de grupos *crackers*. El único objetivo de sus miembros era piratear juegos y otros programas en cuanto salían al mercado para poder presumir de sus habilidades delante de sus colegas.

Había nacido el submundo cibernético. Pronto empezaría a fragmentarse en distintas comunidades; algunas buenas, otras malas.

11

CAMINO SIN RETORNO

Casi dos décadas después de que MiCe! pirateara su primera cinta de casete, el joven Matrix se enfrentaba al mismo dilema. Era adicto a los videojuegos, pero no podía permitírselos. El problema era el mismo, pero la tecnología había avanzado hasta extremos inconcebibles. Los juegos tenían unos gráficos de una sofisticación impresionante, guiones intrincados y retos de una dificultad endiablada.

En muchos casos, la obsesión de los jugadores había sufrido un aumento paralelo. Las cintas y los disquetes ya eran piezas de museo, y los CD-Rom, los DVD y los lápices de memoria (que ni siquiera se habían inventado) pronto quedarían también obsoletos. Cada vez había más juegos que existían simplemente como códigos en la red, pero los equipos domésticos no tenían capacidad para almacenar muchos. Además, era la época de los módems de línea conmutada, cuando conectarse a internet significaba mantener ocupada la línea telefónica durante horas. Claro que algunos sabían cómo acceder desde su ordenador personal a otro mucho más potente, donde podían almacenar y compartir todos los juegos que quisieran…

El acrónimo fXp significa protocolo de intercambio de archivos (*file exchange protocol*), pero basta con saber que los fXp son lo que permite transferir datos entre equipos a gran velocidad. Su mayor utilidad es el intercambio de datos entre servidores. Importa aclarar aquí que un servidor no es más que un ordenador adaptado para hacer las veces de nodo de comunicaciones. Así, por ejemplo, una gran compañía dispondrá de su propio servidor para proporcionar acceso a internet a sus empleados. Muchos servidores son tan grandes y potentes que no dependen de las líneas telefónicas para acceder a la red.

Los paneles de mensajes de fXp congregaron a una fraternidad de usuarios aficionados a piratear servidores con el fin de utilizarlos para almacenar videojuegos y jugar con ellos. Matrix aprendía rápido y, al poco tiempo, su ordenador ya escaneaba la red en busca de servidores.

A través de un programa automático, su equipo esparcía por la red miles de mensajes programados para llamar a la puerta de multitud servidores de cualquier lugar del mundo. Cuando el servidor respondía, el ordenador de Matrix preguntaba: «¿Puedo entrar?». Entonces, la mayoría de los servidores le contestaban: «¿Cuál es la contraseña?». El caso es que se las arregló para encontrar un número suficiente de servidores cuyos administradores no se habían molestado en introducir una contraseña, en cuyo caso el servidor le respondía al equipo de Matrix: «Por supuesto, adelante. ¡Haz lo que quieras conmigo, chico malo!».

Matrix sentía un profundo desprecio por los administradores que dejaban sus equipos indefensos. Cualquiera podía entrar en ellos y robar los datos de una compañía. Para él, era lo mismo que dejar una billetera rebosante de dinero en pleno centro comercial y marcharse.

También había servidores cuya contraseña podía adivinarse sin dificultad, como los que conservaban la que venía de fábrica, por lo común palabras como «admin» o —la más lacerantemente estúpida de todas las contraseñas— «password».

Otros ordenadores tenían fallas en su sistema de seguridad (por ejemplo, un «puerto» o punto de entrada poco utilizado que no requiriese contraseña) susceptibles de ser utilizadas para acceder al servidor. A la mayoría de los usuarios, todo eso les sonaba a chino, pero para Matrix era pan comido y, además, en media hora podía enseñarle a cualquiera cómo se hacía.

Lo primero que Matrix tenía que hacer cuando conseguía controlar el servidor era reparar los puntos débiles de los que él mismo se había servido: debía asegurarse de que nadie más pudiera atacar por la misma vía.

Una vez dentro de un servidor, tenía poder sobre él. Si lo deseaba, podía leer el correo y el tráfico de datos entrantes y salientes. Pero su objetivo era otro: él lo que quería era utilizar los servidores para recibir, almacenar y distribuir juegos mediante la tecnología fXp.

Matrix solo tenía quince años, pero sabía cómo entrar y salir de muchas zonas de internet que la mayoría de los adultos ni siquiera saben que existen. Sus padres no tenían ni idea del mundo secreto que su hijo exploraba desde su cuarto y era improbable que llegaran a descubrirlo. Descargar juegos y programas constituía una ilegalidad flagrante y vulneraba las leyes de propiedad intelectual, pero por entonces era una práctica restringida a un número muy reducido de usuarios. Para los productores representaba una molestia, pero no un problema grave. La inmensa mayoría de los juegos se

adquirían de forma absolutamente legal en las tiendas o en webs como Amazon.

Matrix ocultaba a sus padres lo que hacía no por miedo a infringir las leyes de propiedad intelectual, sino porque, para un adolescente, la maravilla de internet es que sus padres nunca tienen (ni en muchos casos pueden tener) la más remota idea de lo que hace su hijo. Bastante tenían los padres con vigilar qué DVD entraban o salían de casa. Pero los DVD por lo menos eran objetos físicos que un progenitor podía confiscar si, pongamos un ejemplo, sorprendía a su hijo de trece años viendo una película X (a riesgo, por supuesto, de provocarle un incómodo berrinche).

Con internet cambió todo. Los niños empezaron a crecer en un entorno cibernético que para ellos resultaba normal y autosuficiente, pero que los padres veían como algo cada vez más incomprensible y peligroso. Los adolescentes se daban perfecta cuenta de que sus padres, en ese medio, se movían a la deriva. Eso, a su vez, consolidó la idea de que la red era una parcela de sus vidas de la que sus padres podían ser proscritos con toda legitimidad. ¿Cuántos padres y madres han entrado en la habitación de sus hijos y han visto cómo estos minimizaban la ventana del navegador a la vez que se les sonrojaban las mejillas? Basta que un padre eche un vistazo al perfil de Facebook de su hijo cuando este se conecta desde el salón de casa para que el muchacho se transforme en un activista por los derechos humanos y acuse al atribulado progenitor de actuar como un agente de la Gestapo.

Lo que muchos niños y adolescentes no sabían era que, aunque a sus padres pudieran pegársela, había mucha gente —cada vez más— a la que no era tan fácil tomarle el pelo. Entre ellos, acosadores, publicistas, chantajistas, pederastas, policías, profesores y criminales. Solo los usuarios más sofisticados consiguen ocultar a qué se dedican en la red.

A diferencia de los sufridos padres, esas otras personas pertrechadas con un mínimo de conocimientos informáticos empezaban a seguir las huellas digitales que niños y adolescentes habían ido dejando con el paso del tiempo. Tras de sí dejaban confesiones en las que admitían haber tomado drogas y alcohol, insultado a profesores, acosado a compañeros de clase y, cada vez más a menudo, fotografías de sí mismos en actitud pornográfica. Quizá sus padres no supieran nada al respecto, pero otras personas sí estaban al corriente. A veces, incluso un chico listo como Matrix podía pecar de confiado.

Matrix no infringía ninguna ley por el hecho de apropiarse de servidores mal protegidos y destinarlos al almacenaje y uso de videojuegos. A finales del

pasado siglo, Alemania no tipificaba tal cosa como delito, y la cuestión de la propiedad intelectual en la era digital seguía envuelta en brumas, a pesar de que muchos adolescentes y jóvenes adultos empezaban ya a compartir archivos de música a través de Audiogalaxy y Napster. Estas webs redirigían al usuario que quisiera descargarse, por ejemplo, «Bohemian Rhapsody» de Queen hacia ordenadores de cualquier lugar del mundo que tuvieran almacenada la canción. Usando la web como puente, el usuario podía descargarse una copia en su propio equipo.

En un brevísimo espacio de tiempo, millones de personas dieron por hecho que ya no había por qué volver a comprar grabaciones musicales: ¡todo podía encontrarse gratis! Si para el sector de los videojuegos compartir archivos no representaba más que una molestia, para la industria musical se convirtió en todo un desafío. Para atajar el problema, los juristas tenían que redefinir el concepto de propiedad intelectual en la era digital; a continuación, había que persuadir a los legisladores para que promulgasen leyes en ese sentido; por último, había que convencer a las fuerzas del orden de que la detención de piratas digitales era responsabilidad suya. Además, el sector de la música se vio obligado a desarrollar nuevos dispositivos anticopia (empeño en el que han fracasado de forma rotunda una y otra vez).

La costumbre de compartir archivos de música, ligeros y fáciles de transferir entre equipos, se extendió como un reguero de pólvora. Las ventas de música en Estados Unidos alcanzaron su cénit en 1999 con catorce mil millones de dólares; al año siguiente, empezaron a caer, y desde entonces se ha mantenido esa tónica.

Paralelamente, la descarga no autorizada de juegos, cuya extensión es mucho mayor, no repercutió apenas en las ventas de CD-Rom y DVD, que siguieron aumentando de año en año. Las descargas, en todo caso, ayudaron a dar publicidad a los juegos. Con los datos en la mano, lo peor que puede decirse de la actividad cibernética de Matrix es que le quitó horas de sueño y tiempo para hacer los deberes.

Fue entonces cuando Matrix, sin apenas darse cuenta, dio un pequeño paso adelante en la espiral delictiva.

La industria publicitaria había descubierto internet y, como todo el mundo, intentaba averiguar cómo sacarle el máximo partido. La red ofrecía claras ventajas a los publicistas: en primer lugar, permitía identificar al público potencial con mucha mayor precisión. Si una empresa quiere vender pañales, lo que tiene que hacer es olvidarse de las páginas sobre paracaidismo y concentrarse en los foros para padres jóvenes. Si una empresa paga por

anunciarse en televisión, radio o vallas publicitarias, su mensaje llega también a los paracaidistas, cosa que no tiene mucho sentido (a no ser, claro, que el paracaidista en cuestión acabe de ser padre).

En segundo lugar, internet permite calibrar el éxito y el coste de la publicidad. Cada vez que un padre o madre hace clic en el anuncio de pañales, queda registrado en los archivos del fabricante y de la empresa de publicidad. La empresa, pues, recibe una remuneración en función del número de clics. Productores y publicistas pueden analizar el llamado ratio de clics (CTR, por sus siglas en inglés) para que el fabricante de pañales pueda comprobar que, de cada cien visitantes de la página de paracaidismo, ni uno solo se interesó por el anuncio, que en cambio fue visitado por diez de cada cien visitantes en el foro de padres, lo que da como resultado un CTR del diez por ciento y permite que la empresa publicitaria sea remunerada de forma acorde. El problema fue que en poco tiempo el CTR dio paso al fraude de clics.

El administrador de uno de los foros frecuentados por Matrix estaba implicado en un caso de estafa. El administrador animó a Matrix a utilizar los servidores bajo su control para instalar un programa que, de forma automática, hacía clic a intervalos en determinados anuncios. Con cada clic, ganaba un centavo. El muchacho ni siquiera sabía que eso era ilegal. Luego el administrador le aconsejó consultar otro foro donde se discutían temas parecidos, y fue en ese foro, Carder Planet, donde por primera vez oyó hablar del fraude con tarjetas de crédito.

Matrix atravesó el Rubicón en estado de trance, sin darse cuenta de que a su alrededor las aguas formaban remolinos. Todavía era un chiquillo, pero poco a poco iba hundiéndose en el tremedal de la delincuencia. Es posible que, en su interior, algo le dijera que aquel era un mal camino, pero en el ciberespacio las fronteras son borrosas, cuando no invisibles.

12

PASAJE A LA INDIA

Chennai, Tamil Nadu, 2001

En 2001, Renu llevaba nueve años sin ver a sus padres y hermanos. A veces, hasta los jóvenes que como Renu han aprendido a sobrevivir con vínculos familiares más bien débiles se sienten obligados a atender los ruegos de una madre. Tras mucho discutir, le prometió que conseguiría el dinero necesario para volar a Tamil Nadu, en el sur de la India, y visitar a la familia.

Pero reunir el dinero no era fácil. Durante su época de estudiante en la Universidad de Westminster, Renu había trabajado como repartidor en Pizza Hut. Trabajaba hasta las doce o la una de la noche y tenía que madrugar para asistir a la primera clase de la mañana (aunque con el tiempo su puntualidad fue disminuyendo). Gracias al trabajo, por primera vez en su vida disponía de algo de dinero, pero no bastaba para ahorrar: lo poco que le sobraba lo gastaba en su adicción a las drogas. Por entonces consumía cocaína y poco después se pasaría al devastador crac.

Al ver que no podía reunir la cantidad necesaria, Renu pidió prestado a sus amigos y, por seguridad, antes de emprender el largo vuelo hasta Chennai, adquirió tres mil libras en cheques de viaje de American Express.

Nadie sabía muy bien qué esperar de aquel encuentro: se había separado de su madre en su infancia, y ahora era un joven adulto con una vida marcada por periodos de intensa soledad. Su vida social había mejorado desde los años de instituto, pero le costaba mantener conversaciones de circunstancias o dar grandes muestras de emoción. Además, a pesar de su juventud, su pasado empezaba a componerse a base de retazos. Había muchas cosas que no estaba dispuesto a compartir con su familia.

El viaje empezó con mal pie. En Chennai tenía que tomar uno de los atestados e incómodos autobuses que cubren las rutas rurales, lo que suponía compartir espacio con demasiadas personas, aparte de gallinas y equipajes. Estaban a medio camino y los ojos empezaban a cerrársele por el largo viaje desde Londres cuando un leve golpe lo hizo despertar un instante. En ese

momento no le dio mayor importancia, pero la alegría del reencuentro con la madre quedó empañada al bajar del autobús y descubrir que le habían rajado la bolsa y que las tres mil libras en cheques de viaje habían volado.

Lo peor estaba por llegar. Cuando se presentó en las oficinas de American Express en Chennai, el personal se negó a reembolsarle el dinero. (A su entender, ese era el sentido de preferir los cheques al metálico). Si quería otro talonario, tendría que presentar una confirmación escrita de la policía local de que el talonario le había sido robado. Aun así, le advirtieron, Amex no garantizaba la devolución del dinero, sino que se lo abonaría «a su discreción».

Ya en Inglaterra, los burócratas de Amex lo recibieron con el mismo ademán impasible. Se empeñaban en que Renu no había aportado la documentación requerida para demostrar que los cheques habían sido robados o perdidos. Por consiguiente, no podían devolvérselos.

Las personas que le habían prestado dinero eran amigas, pero hasta un punto. Se hacían cargo de la situación de Renu, pero querían su dinero. La única manera de devolverlo era hacerse con una tarjeta de crédito; después de todo, vivían en la era del plástico y los bancos y las compañías de crédito estaban dispuestos a aceptar a todo el mundo como cliente, hasta a Renu.

El tedioso trabajo en Pizza Hut no daba para cubrir sus crecientes necesidades económicas: la deuda, la bebida, las drogas, los gastos de la universidad, el alquiler. El mundo de Renu empezaba a desmoronarse. Lo primero que se resintió fueron las tareas de la facultad. Tras superar los exámenes del primer año en el campus de Harrow de la Universidad de Westminster, Renu empezó a faltar a clase. Suspendió los exámenes del segundo año, y también las recuperaciones.

Para evadirse de su desesperación, empezó a descargar compulsivamente canciones por Napster, y poco después descubrió las webs donde los miembros de la Escena compartían los juegos y programas que ellos mismos pirateaban. Las noches eran cada vez más largas y Renu las dejaba pasar sumergido en el mundo seguro y distante de la pantalla luminosa, lejos de los zarpazos de la dura realidad.

Una noche, le explicó la historia de los cheques perdidos a uno de los muchos navegantes itinerantes que conocía por la red y el canal de IRC. «Pásate por amexsux.com —le dijo el contacto—. ¡Por lo menos, te sentirás mejor!».

A Renu le encantó la web (lema: «Sal de casa sin ella»). En ella, los antiguos clientes de American Express se desahogaban denunciando

supuestos abusos. La animadversión hacia la compañía está bastante generalizada, como puede comprobarse haciendo una búsqueda en Google: existen cientos de páginas dedicadas a despotricar contra Amex, muchas de ellas con profusas listas de enlaces a noticias negativas sobre la empresa.

Uno de los participantes había colgado en el panel de mensajes una propuesta abierta a todo el que tuviera motivos de queja contra la compañía: «¡Véngate! ¡Visita CarderPlanet.com!».

Nada más zarpar con rumbo a Carder Planet, Renu sintió que había llegado el momento de decir adiós a su vieja personalidad. Fue así como se convirtió en JiLsi y se puso como avatar la cara de un pirata gamberro de dibujos animados con sombrero rojo y parche negro en el ojo izquierdo. Cual Jack Sparrow en pleno Caribe cibernético, Renu no tardó en sentirse a gusto entre aquel infame grupo de *hackers*, *crackers* y estafadores, y enseguida decidió fondear en Carder Planet. Por algún lugar de aquel grupo de inadaptados merodeaba Matrix, y, aunque todavía faltaban unos cuantos meses para que se profesaran voto de amistad virtual, ambos se convirtieron en dos nombres habituales en los millares de páginas que trataban de emular a Carder Planet.

¿Dónde se ha visto a un refugiado drogadicto de Sri Lanka confraternizando con un recatado adolescente alemán de clase media gracias a la hospitalidad de un carismático odesita con una visión propia de la nueva Ucrania? ¿Dónde sino en la red?

13

AL ROJO VIVO

Nueva York, 2003-2004

RedBrigade decidió que había llegado el momento de ir a por Washington Mutual: para él, no era más que un proveedor de dinero gratuito. El banco había perdido su condición de cooperativa de ahorro en 1983 y ahora su consejero delegado anunciaba su intención de convertir la venerable institución de Seattle en «el Wal-Mart de los bancos». La filosofía de la dirección era arramblar con todo lo posible: vender préstamos sin preocuparse por los activos, los pasivos ni el sueldo de los clientes; juntar las hipotecas basura en paquetes para moverlas mejor; invertir lo mínimo imprescindible en equipo y personal. Una banca de bajo coste; lujos, los justos. Por suerte para RedBrigade y sus colegas, la partida de gastos no incluía ni siquiera las medidas de seguridad más elementales.

RedBrigade salió del hotel Four Seasons en la calle 57 cerca de la Quinta Avenida hacia las once de la mañana. Todavía estaba algo aturdido por la fiesta de la noche anterior, pero a fin de cuentas había consumido champán añejo y cocaína casi pura, así que se sentía en plenas condiciones para entrar en combate.

Ya en la sucursal, se acercó a una de las inexpertas cajeras («así no tienen que pagarles tanto») y le extendió su tarjeta de débito.

«¿Cuánto desea hoy, señor?».

«Diez mil, por favor».

«¡Marchando!».

Tac-tac-tac, tac-tac-tac. Para sacar dinero en Washington Mutual, RedBrigade tenía que entregar su tarjeta a la cajera para que esta la deslizara por un lector. En cualquier otro banco, tal vez el empleado habría visto entonces un mensaje en código advirtiéndole de que había saltado la alarma y RedBrigade habría tenido que descifrar la expresión del rostro de la cajera: ¿Me habrá descubierto? ¿Salgo corriendo? ¿Me quedo aquí como un idiota y espero a que llegue la policía? Quizá no pasa nada, ¿estaré paranoico?

Pero en Washington Mutual no. Por pura avaricia, la directiva creía que podía pasarse sin pantallas de ordenador ni mensajes de seguridad codificados. Así pues, si la sucursal rechazaba la tarjeta, RedBrigade se limitaría a poner cara de sorpresa, disculparse y desaparecer. En Washington Mutual nunca se llamaba a la policía.

Pero sus tarjetas nunca fueron rechazadas. Aquel día de diciembre de 2003, la mujer deslizó la tarjeta, la operación fue aprobada al instante y, a continuación, le hizo firmar un recibo con el código de la transacción. Luego él se dirigió al cajero automático situado en la parte delantera del banco e introdujo el código. Un momento de espera y, acto seguido, como si de una tragaperras mágica de Las Vegas se tratase, empezaron a llover billetes de cincuenta dólares: mil, dos mil, tres mil… RedBrigade recogió los doscientos billetes todavía frescos y se los enfundó en el bolsillo.

A veces era como si los bancos hubieran dejado los cajeros automáticos abiertos a propósito para él y sus colegas. Era tan fácil que parecían los elegidos. Él disfrutaba sobre todo exprimiendo los cajeros de Citibank. Si un banco se lo merecía, ese era el Citi. En primer lugar, era el más inmoral de todos aquellos bancos espurios. En segundo lugar, sus medidas de seguridad eran penosas.

El *phishing* fue, desde buen principio, una estrategia crucial en todas las ramas de la delincuencia informática. Por rígidas que fuesen las defensas digitales de una compañía, cualquier *hacker* con un mínimo de experiencia podía burlarlas si atacaba por la vía del *phishing*. El asunto consiste en realizar un envío masivo de correos electrónicos a direcciones pertenecientes a una determinada empresa —por ejemplo, un banco— o, en ocasiones, al azar. A menudo, los correos basura contienen archivos adjuntos infectados o enlaces que, al hacer clic en ellos, redirigen a webs desde las que se descarga *malware*. Si un *hacker* envía varios millones de correos basura, basta con que le respondan a unos pocos para que la operación tenga éxito; los ordenadores infectados le permiten acceder a cuentas bancarias y demás información de tipo personal o financiero.

La seguridad de los bancos siempre ha tenido un gran enemigo: sus clientes (aunque esto no es excusa para justificar los pésimos sistemas de seguridad empleados por los bancos durante los primeros quince años de banca electrónica). Los mejores sistemas pueden hacer aguas por culpa de una sola pieza, y nosotros, los cientos de millones de usuarios, somos esa pieza.

Así pues, cuando un banco es inexpugnable, el ciberladrón recurre a los clientes en busca de ayuda. Envía a los titulares de las cuentas millones de

correos electrónicos que parecen remitidos por el banco y espera a que respondan: al poco tiempo, recibe una avalancha de números de cuenta y contraseñas.

Estafar a los clientes de Citibank era un juego de niños:

> Comprar direcciones de correo recién pirateadas. Hecho.
>
> Comprar Dark Mailer, el sueño de todo *spammer*. Hecho.
>
> Comprar *proxies*. Hecho.
>
> Comprar alojamiento. Hecho.
>
> Diseñar una nueva página de Citibank. Hecho.
>
> Añadir una ventana que no desaparezca hasta que se introduzca el número de tarjeta y el PIN correspondiente. Hecho.
>
> Crear una dirección de correo electrónico para recibir números de cuenta y contraseñas. Hecho.

RedBrigade dedicaba unas horas cada día a su labor. Estudiaba los detalles de cierta doctora H. M. Hebeurt del norte del estado de Nueva York. «Hmm… Vive cerca. ¡La hostia, gana cincuenta mil al mes y el marido, más de setenta y dos mil!». Investigando un poco más, descubría que su objetivo trabajaba en Wall Street. Tal vez, pensaba, si su vida hubiera seguido otros derroteros, podría dedicarse a robar de forma legal, como ese tipo… Pero no había tiempo para fantasías, tenía que hacer cálculos. Veamos: dos cuentas corrientes, dos cuentas de ahorro, una cuenta de descubierto y una tarjeta de crédito… dos mil dólares de cada una. Total, doce mil dólares de un plumazo.

Cada día llegaban a su bandeja quince mensajes como ese.

Las visitas al Washington Mutual de Nueva York se repitieron durante algo más de quince días y generaron casi trescientos mil dólares. No era tanto, teniendo en cuenta que sus gastos semanales eran del orden de los setenta mil. Cada dos o tres meses, compraba un Mercedes o un BMW nuevo de alta gama. Viajaba siempre en primera. Compraba relojes Breitling de diez mil dólares como quien compra el periódico. Disponía de un apartamento formidable en el Upper East Side, pero solo pasaba en él dos o tres noches por semana porque prefería los hoteles de lujo de la ciudad. RedBrigade ganaba más dinero que una estrella del fútbol en Inglaterra, y además sin impuestos del 50 por ciento.

No había nada que no pudiera permitirse. Cada vez que sacaba sus fajos de billetes de cincuenta, se quedaba mirando la cara de los dependientes, que debían de preguntarse quién era. Debían de tomarlo por un *hippy* de familia

bien o por un traficante. De todos modos, los multimillonarios de la era del plástico se dejaban ver tanto en vaqueros y camiseta como con un traje Savile Row. Sea como fuere, los vendedores —joyeros, encargados de concesionarios, vinateros, hoteleros— siempre aceptaban su dinero sin hacer preguntas. Nunca se sabe: ¿y si ese tipo con las mejillas sin afeitar trabajaba en Google? Además, ¿qué más daba cómo hubiera ganado ese dinero?

Solo había un problema: tenía demasiado dinero en metálico. Una tarde llegó a casa con setenta y siete mil dólares en el bolsillo, a sumar a los trescientos mil que ya había en el apartamento. Aparte, tenía otros ciento diez mil en giros postales. RedBrigade había organizado un operativo global para retirar dinero: él enviaba las tarjetas y los datos de las cuentas a un intermediario de Europa del Este, y este vaciaba los cajeros automáticos para mandarle el dinero. Después tenía que volver a ingresarlo, y ya estaba harto de las directivas de notificación, según las cuales cualquier transacción superior a diez mil dólares debe ser comunicada al Tesoro en cumplimiento de la legislación contra el blanqueo de capitales. «¡Mierda —pensaba—, quién podía imaginar que iba a ser tan difícil gastar el dinero!».

Estaba a punto de ir a retirar otros setenta y siete mil dólares. No tenía más que caminar unas cuantas manzanas desde su apartamento, pero entonces pensó: «Ya tengo muchísimo dinero encima, paso». Sabía que algo no debía de ir bien. Una idea se repetía en su cabeza: «Carder Planet no está mal, pero Shadow Crew es la leche. ¿Quién iba a creer que podría presentarme día sí y día no en el banco y salir con cincuenta de los grandes en el bolsillo? ¡Es de locos!».

Cuando Carder Planet cerró por fin sus puertas en 2004, podía presumir no solo de alojar foros en ruso y en inglés, sino también secciones en coreano, chino e incluso árabe. «Carder Planet cambió las reglas del juego —asegura E. J. Hilbert, un antiguo agente especial del FBI que dedicó varios años a investigar la web—. Sus sucesores la tomaron como modelo. No es ninguna exageración decir que difundió la delincuencia *hacker* hasta el último rincón del planeta».

Por todas partes empezaron a brotar páginas a imagen y semejanza de Carder Planet: Theftservices.com, Darknet.com, Thegrifters.net, Scandinaviancarding.com. Había muchas otras, incluida una bautizada con un simpático acrónimo a modo de parodia de las comunidades académicas norteamericanas: la IAACA (siglas en inglés de la Asociación Internacional para el Progreso de la Actividad Criminal).

Sin embargo, ninguna cosechó tanto éxito como Shadow Crew durante sus dos años de existencia. RedBrigade fue uno de los muchos tarjeteros que hicieron su agosto con ella. Las fuerzas de la ley empezaban apenas a vislumbrar la magnitud del negocio; los bancos la desconocían; el ciudadano de a pie ni siquiera imaginaba su existencia.

Los *hackers* estaba muy adelantados y la avaricia reinaba en todas partes: gestores de fondos de inversión libre, oligarcas, jeques del petróleo, magnates de la telefonía móvil latinoamericana, la nueva élite negra sudafricana, la antigua élite blanca sudafricana, fabricantes chinos de bibelots globales, gurús tecnológicos trasladados de Bangalore a Silicon Valley.

Cientos de tarjeteros amasaron grandes fortunas con Shadow Crew, pero la ingenuidad de muchos los llevó a despilfarrarlas en lujos de nuevo rico. En aquellos tiempos, nadie registraba la dirección IP de un equipo al realizar transacciones en la red. Tampoco existían los sistemas de verificación de direcciones de las tarjetas de crédito: independientemente de en qué país se hubiera emitido la tarjeta, cualquiera podía comprar productos en cualquier parte del mundo (excepto en Rusia y otros países exsoviéticos) sin miedo a que nadie cruzara los datos en ningún momento.

Esta nueva modalidad de delincuencia arraigó con fuerza más allá de la cuna rusoucraniana. Su globalización fue espontánea. RedBrigade recuerda cómo delincuentes asiáticos de renombre empezaron a entrar en contacto con universitarios de Massachusetts que, a su vez, mantenían relación con europeos del Este, cuyos ordenadores rebosaban datos de tarjetas de crédito. Detrás de algunos de los alias de Shadow Crew se escondían grupos criminales como All Seeing Phantom, muy respetado en su entorno.

RedBrigade, diez años mayor que casi todos los miembros de Shadow Crew, no le encontraba sentido a intentar escalar puestos en la jerarquía para granjearse el reconocimiento y el respeto de sus colegas. No entendía por qué la mayoría de los miembros mostraban aquel temor reverencial hacia los moderadores y los administradores de los foros. Por grande que fuera su éxito, los administradores de Shadow Crew tenían comportamientos inmaduros, casi infantiles, lo cual no es de extrañar si se piensa que la mayoría rondaban la veintena. RedBrigade era consciente de que Carder Planet había sido creada y desarrollada por delincuentes de verdad, en tanto que muchos de los integrantes de Shadow Crew no eran más que diletantes que engordaban su infinita vanidad a base de las formidables sumas de dinero que ganaban.

Cuanto más equidistante se mantuviera de esos individuos, menor sería el riesgo de ser identificado por las fuerzas del orden. A excepción de una minoría, los miembros de Shadow Crew ignoraban que el Servicio Secreto había conseguido penetrar muy hondo en la web.

En abril de 2003, había sido detenido Albert Gonzalez, un joven estadounidense de origen cubano y uno de los miembros más veteranos de Shadow Crew. Entre los tarjeteros se lo conocía como CumbaJohnny. Lo que nadie sabía era que tras su arresto se había convertido en confidente, y gracias a él el Servicio Secreto hizo grandes progresos. Gonzalez dirigía una red privada virtual (RPV) a través de la cual se comunicaban los pesos pesados de la página. Si una RPV se mantiene de forma adecuada, es muy difícil, si no imposible, que la policía llegue a detectarla; a menos, claro, que el administrador de administradores esté a la vez al servicio de la policía, como en el caso de Gonzalez.

El 26 de octubre de 2004, el Servicio Secreto estadounidense llevó a cabo una serie de redadas por todo el país que se saldaron con el arresto y posterior procesamiento de diecinueve personas por su implicación en Shadowcrew.com. Con el tiempo, aumentaría el número de detenidos.

«Shadow Crew —se lee en el auto de procesamiento por conspiración— era una organización internacional de aproximadamente cuatro mil miembros que promovía y facilitaba una amplia variedad de actividades criminales». El joven equipo de ciberpolicías del Servicio Secreto había cobrado una buena pieza. La acusación, presentada ante el tribunal del distrito de Nueva Jersey, era muy explícita: «Los administradores —continúa— controlaban de forma colectiva la dirección de la organización y decidían sobre su funcionamiento cotidiano, así como sobre los planes para su viabilidad a largo plazo […]. Los administradores gozaban de acceso sin restricciones a los servidores informáticos donde se alojaba la web de Shadow Crew y, por consiguiente, eran los responsables últimos de la administración física, el mantenimiento y la seguridad de dichos servidores, así como del contenido del sitio web».

Los medios se volcaron exaltados en la noticia de la desarticulación de Shadow Crew. Incluso llegaron a sugerir que la operación equivalía, en el mundo virtual, a la caída del clan de los Corleone en Sicilia. La cobertura fue tan vasta en parte porque una de las acusadas era una mujer, Karin Andersson, alias Kafka, aunque lo que el Servicio Secreto no sabía era que, en realidad, el delincuente era su novio, que utilizaba el ordenador y la dirección IP de la muchacha para cometer sus fechorías. Nada extraordinario, si se considera que el 96 por ciento de los *hackers* son hombres.

Las detenciones, sin duda, tenían fundamento. Pero ¿eran los «administradores» quienes ganaban dinero con Shadow Crew? En realidad no, si bien es cierto que entre ellos se contaban algunos de los llamados «monetizadores» (el primero, Gonzalez, quien, a pesar de su estrecha vinculación con el Servicio Secreto, terminaría cometiendo una estafa aún mayor al apropiarse de la base de datos de tarjetas de crédito de T. J. Maxx).

La policía se enfrentaba a un problema que se convertiría en recurrente: los *hackers* no eran delincuentes ordinarios. Es cierto que los auténticos delincuentes se sirven de sus habilidades para cometer delitos reales contra personas de verdad. Pero los *hackers* a menudo pasan por alto esa faceta de su actividad. Son los «lobos solitarios» de Script, personas a quienes, a menudo, lo que les interesa no es amasar fortunas, sino distinguirse como maestros dentro de su grupo de colegas. «Hay que entender —explica JiLsi al recordar su época de tarjetero— que todo aquello era un juego. Era como jugar al Grand Theft Auto, solo que las consecuencias eran reales. Los policías a los que nos enfrentábamos eran personas de carne y hueso. ¡Eso lo hacía mucho más emocionante! Es una cuestión de respeto. Es una cuestión de… —Pausa dramática de JiLsi— reputación».

En un sentido, no obstante, la redada contra los miembros de Shadow Crew sí tuvo efectos equivalentes a los de la caída de una organización mafiosa en el mundo real: provocó un vacío de poder y desató una lucha sin cuartel por la supremacía entre la siguiente generación de tarjeteros, que se agruparon en torno a dos nuevas páginas webs aparecidas al año siguiente: Carders Market y Dark Market.

PARTE IV

14

EL REPARTIDOR DE HIELO

Santa Clara, California, octubre de 1998

Max Vision se quedó de una pieza cuando vio aparecer a Chris y Mike, sus dos contactos de la sede del FBI en San Francisco, en la puerta de su casa de Santa Clara. No reconoció al hombre que iba con ellos, aunque más tarde supo que era el jefe de la división de crímenes informáticos del FBI. Pero aquella no era una visita de cortesía: «Vamos a presentar cargos contra ti, Max —dijeron—. Esta vez la has cagado».

Sin saber muy bien qué decir, Vision les entregó su ordenador y todo lo demás; no quería dar la impresión de estar obstruyendo la justicia y, a la vez, no tenía muy claro cuál era el problema.

Llevaba una vida correcta, ejemplar incluso. Después de una adolescencia difícil en Iowa, se trasladó a una región donde la gente no se escandalizaba al cruzarse con un *geek* con las greñas recogidas en una cola de caballo. Nadie le dio tampoco la menor importancia al hecho de que cambiase su prosaico apellido, Butler, por el de Vision. Pronto se acostumbró a la vida indolente de la Costa Oeste y, para rematarlo, estaba profundamente enamorado de Kimi, su prometida.

A sus veintiséis años, Max Vision era un genio de la seguridad informática y uno de los consultores más respetados y valorados del área de la bahía de San Francisco. Además, era un tipo con vocación cívica, creador de la página web Whitehats.com, destinada a ayudar a particulares y empresas a blindarse contra ataques cibernéticos. En ella, Vision informaba sobre las vulnerabilidades de ciertos programas de uso corriente y explicaba cómo parchearlas.

Los *hackers* se relamen cuando encuentran vulnerabilidades, ya que representan su principal ruta de acceso a los equipos de terceros. Son como agujeros digitales en la armadura de los programas y los sistemas, vacíos que el fabricante no ha previsto. Cuando una compañía como Microsoft o Adobe descubre que un *hacker* ha penetrado en Windows o en una aplicación tan

omnipresente como el PDF Reader sirviéndose de una determinada vulnerabilidad, puede cerrarla o parchearla confeccionando los llamados ajustes de seguridad específicos. A continuación, la empresa avisa a sus clientes para que descarguen el parche y lo instalen, bloqueando así esa ruta de acceso al equipo del usuario. Si el usuario no instala la actualización, su ordenador seguirá siendo vulnerable a los virus que explotan ese defecto.

Algunos superexpertos en seguridad, como Vision, son los primeros en identificar los puntos vulnerables y, como buenos samaritanos, ofrecen consejos prácticos a los usuarios para que puedan protegerse.

Pero Vision fue todavía más allá en su altruismo; un buen día se puso en contacto con la sede del FBI de San Francisco para ofrecerles sus servicios de forma gratuita, a lo que los federales accedieron encantados.

Para Max Vision, no había en la red desafío insuperable ni vulnerabilidad invisible. Pero, para descubrir esos flancos débiles, primero tenía que explorar a fondo los sistemas, y eso lo colocaba en el epicentro de un profundo dilema que no solo afectaba a la industria informática, sino que tenía importantes ramificaciones. A veces, para estar protegido contra los *hackers* perniciosos o «de sombrero negro», es necesario que un *hacker* «de sombrero blanco» aprenda a introducirse en los sistemas, lo que en sí mismo puede constituir una ilegalidad.

Es poco menos que inevitable que los «sombreros blancos», al igual que los «sombreros negros», inspeccionen los grandes sistemas informáticos públicos. La diferencia reside en que los primeros no aprovecharán en beneficio propio las vulnerabilidades que encuentren; los segundos es probable que sí.

Vision, que trabajaba desde la pequeña casa que compartía con Kimi, se dio cuenta de que, cuando daba con una anomalía o un problema, no podía resistir la tentación de corregirlo. En 1998 descubrió un peligroso defecto en las redes que prestaban servicio a varios organismos del gobierno, entre ellos parte del Pentágono. Aquello representaba un agujero en sus defensas a través del cual podían deslizarse todo tipo de temibles gusanos. Cualquier *hacker* de cualquier lugar del mundo con conocimientos suficientes podía poner en riesgo literalmente cientos de miles de ordenadores del gobierno. Demostrando una vez más su compromiso patriótico, Vision rellenó esos agujeros con cemento digital con el propósito de reafirmar la seguridad de su país: nadie podría volver a explotar esa vulnerabilidad, al menos no en esos departamentos gubernamentales.

A partir de ese día, todo cambió.

Tanto entonces como con la perspectiva del tiempo, la acción de Vision parece insignificante. Su intervención fue tan minúscula y fugaz que apenas dejó rastro: un impulso electrónico casi inapreciable; un golpe de tecla; una letra entre páginas y páginas de código informático; el reflejo condicionado de un *hacker* nato. Sin embargo, Max Vision dejó abierto un diminuto agujero por el que solo él habría sido capaz de entrar. Poco después, un agudo ciberinvestigador de las fuerzas aéreas estadounidenses lo descubrió y resiguió su origen hasta dar con el responsable.

Ese era el motivo que había llevado a sus amigos del FBI a llamar a la puerta de su casa de Santa Clara. Era el primer indicio de la tormenta que se avecinaba. «Nos has causado un montón de problemas, Max —dijeron—. Es un asunto de seguridad nacional, por eso las fuerzas aéreas han tomado cartas en el asunto».

Vision estaba molesto e indignado. Había advertido por correo electrónico a las autoridades con anticipación, confiándoles sus sospechas acerca de la vulnerabilidad del sistema y su intención de escanearlo a modo de comprobación.

¿Cuán grave era un delito como ese? Sus acciones no obedecían a fines económicos ni perseguían ningún otro tipo de beneficio. Al contrario, había hecho un favor considerable a los organismos federales implicados. Entre otras cosas, Vision había reforzado la seguridad de los sistemas informáticos de bases militares y centros de investigación nuclear, como los laboratorios nacionales de Brookhaven y Livermore. Puesto que el daño ocasionado había sido mínimo y que no había robado nada, ¿qué sentido tenía detener por ello a uno de los informáticos mejor dotados del continente?

El descubrimiento de las fuerzas aéreas no solo condujo al arresto de Max Vision bajo la acusación de haber instalado un gusano peligroso. Las consecuencias fueron aún más graves, pues aquel pequeño agujero abierto en los puertos de entrada de la red informática creció y creció hasta convertirse en un tenebroso abismo: la Institución Correccional de Taft, una prisión federal situada en el desierto que se extiende al norte de Los Ángeles. Vision fue a prisión por ser un *hacker* hábil y consumado, no por ser un delincuente. Todo lo que sabía sobre delincuentes profesionales era lo que le explicaban sus contactos del FBI. Pero pronto eso iba a cambiar; Max ingresó en una prisión de baja seguridad con un gran número de reclusos condenados por fraude y demás delitos financieros.

Se hallaba en una tesitura difícil, pero todavía iba a empeorar. Lo condenaron a dos años de internamiento en Taft, y, al mes de ingresar, Kimi

le hizo saber que rompía con él.

Al ver que su mujer lo dejaba por otro hombre y que sus antiguos amigos del FBI se desentendían de él, Max Vision se precipitó a un abismo al fondo del cual aguardaba una profunda depresión. Fue entonces cuando conoció a otro recluso, un tal Jeffrey Normington, que le tendió una mano amiga cuando todo el mundo parecía haberle dado la espalda.

Al salir de la cárcel, Vision no encontró ningún empleo donde pagaran más que el sueldo mínimo. Buscó trabajo y le ofrecieron buenos puestos en compañías de seguridad del extranjero, pero las restricciones de la condicional le impedían obtener el pasaporte, y en Silicon Valley nadie estaba dispuesto a contratar a alguien en cuyo currículo figurase una condena indeleble por delitos informáticos.

Las deudas aumentaban y la desesperación se hacía más profunda. De pronto, un día Normington reapareció y le prometió que lo sacaría del abismo y que volvería a ver el sol de California. El camino estaba sembrado de ganancias. Normington le prometió un portátil Alienware último modelo, herramienta imprescindible aunque costosa. Y eso no era más que el principio. Además, le conseguiría un apartamento y correría con los gastos. Normington se encargaría de todo.

Eso sí, a cambio de algunos favores.

Vision podría haber elegido otro camino. Podría haber explorado otras alternativas. Podría haber recurrido a los amigos o a la familia. Pero estaba agotado, se sentía solo y Normington supo ser persuasivo. Enfrentado al dilema, optó por la vía equivocada.

Max Vision, el benefactor, desapareció en el fondo del abismo, y en su lugar apareció Iceman, el repartidor de hielo, un personaje siniestro con un *alter ego*, Vision, formado al amparo de los federales.

15

CARDERS MARKET

Iceman contempló desde la barrera cómo el Servicio Secreto estadounidense le ganaba la partida a la cúpula de Shadow Crew. No se sentía para nada identificado con aquella panda de impresentables que, mientras desvalijaban a particulares desprevenidos por la red, permitían que confidentes, soplones y *rippers* devoraran por dentro la organización.

Con Shadow Crew fuera de circulación y varios aspirantes rivalizando por ocupar su lugar, Iceman decidió enseñarle al mundo cómo vencer a la ley. Ante todo, lo que quería era demostrar su poder sobre el ciberespacio y sus usuarios.

Para Iceman, las webs de tarjeteros eran emporios anárquicos donde el dinero era lo de menos; lo importante de veras era la libertad de actuación. Estaba sinceramente convencido de que la creación de mercados especializados donde se intercambia información, como en Carders Market, la página que acababa de diseñar, no debía considerarse en sí misma una actividad delictiva, por más que pudiera incitar a algunos de sus usuarios a delinquir. Su web y otras parecidas eran la prueba de que la red, a diferencia de otras parcelas de la vida, no debía estar limitada por la rigidez de la intervención estatal; de hecho, la página principal contenía un mensaje muy directo destinado a policías y administradores de internet:

> MENSAJE PARA FUERZAS DE SEGURIDAD Y PROVEEDORES DE SERVICIOS Y ALOJAMIENTO
>
> Carders Market es un foro **legal** concebido como lugar donde sus miembros puedan debatir sobre temas de su elección. **No** se permiten bajo ningún concepto contenidos ilegales; de hallarlos, el equipo de la web los suprimirá de forma inmediata. Debatir no es delito. Gestionar un foro no es delito. La página no contiene números de tarjetas de crédito, ni cuentas bancarias, ni pornografía, ni virus, ni nada susceptible de ser considerado ilegal en Estados Unidos ni en el resto de la comunidad

> internacional. Los negocios que puedan llevar a cabo nuestros miembros **no son de nuestra incumbencia** y, en cualquier caso, se desarrollan **fuera del foro**. No aprobamos las actividades ilegales y en ningún caso tomamos parte en ellas.

Cuanto más se adentraba en el mundo de las tarjetas, más se enredaba su telaraña moral. Con el nombre de Iceman, Vision nunca compró ni vendió tarjetas de crédito; para ello, creó otro personaje virtual. Algo que todos los *hackers* tienen en común es la facilidad con que compartimentan su personalidad. En ocasiones, Vision parecía creer de veras que sus personajes pensaban y actuaban de forma autónoma, y que por lo tanto conformaban entidades morales distintas.

Como Iceman, su ambición era vencer tanto a sus competidores del sector como a la policía para erigirse así en señor indiscutido del contrabando de tarjetas. Para ello, ideó una estrategia doble. Por un lado, identificar y delatar a los soplones (confidentes) y policías que rondaban los paneles de discusión. Por otro, derrotar a la competencia, es decir, a los demás foros que luchaban por la hegemonía en el sector.

Mucho antes de que el Servicio Secreto planificara el cierre de Shadow Crew, Iceman ya sabía que varios de sus miembros clave eran confidentes de las fuerzas de seguridad de Estados Unidos y Canadá y, en algunos casos, incluso agentes de policía. Quienes como él vivían de engañar a los demás tenían que saber ver cuándo eran los demás quienes intentaban engañarlos a ellos. Si algo tenían claro los ciberladrones y ciberpolicías veteranos, era que nada fomenta la falsedad y la simulación como internet. Para Iceman, detectar soplones formaba parte de su trabajo.

Cuando Iceman descubría a un confidente, colgaba vitriólicas acusaciones contra él en los paneles de mensajes. Algunos miembros empezaron a pensar que Iceman protestaba demasiado. ¿Podría ser que el confidente fuera el propio cerebro de Carders Market? De hecho, eso fue lo que muchos pensaron cuando lo vieron llevar a cabo su plan maestro para barrer a la competencia, una serie de ataques contra foros rivales destinados a eliminarlos y absorber las voluminosas bases de datos de sus miembros. Vision no disimulaba sus intenciones; de todos era conocido el tono arrogante con que proclamaba que otras webs delictivas, como Scandinaviancarding.com o Talk Cash, «no tenían ningún derecho a existir».

Para subrayar su superioridad, creó en primer lugar un rastro digital falso para que pareciera que el servidor de Carders Market estaba localizado en Irán, es decir, fuera del alcance tanto de la policía como de otros tarjeteros. El

servidor, en realidad, se hallaba en California, pero a Iceman se le daban tan bien las mentiras que todo el mundo se convenció de que la web estaba alojada en Irán. Como es natural, eso desató los rumores: ¿sería Iceman un agente de la inteligencia iraní encargado de sembrar la confusión entre las fuerzas del orden estadounidenses y reunir fondos para operaciones encubiertas?

Quienquiera que fuese, era evidente que no se andaba con chiquitas. Una tras otra, logró infiltrarse en todas las páginas rivales y apropiarse de sus bases de datos, donde figuraban las direcciones de correo electrónico y contraseñas de sus miembros, así como el registro de todos los mensajes publicados. Una vez en su poder, vertía toda la información en Carders Market y la borraba del sitio original.

Sus ataques eran implacables, ni siquiera los rusos escaparon a sus iras. Incluso se atrevió a atacar Mazafaka.ru, la emblemática página que había sustituido a Carder Planet en los afectos de la comunidad *hacker* rusa. No obstante, aunque en ocasiones el ego le nublara la razón, sabía muy bien que destruir las webs rusas de la misma manera que había destruido las webs inglesas habría sido una grave imprudencia. Los rusos contaban con algunos de los *hackers* más brillantes del mundo y Iceman no tenía ningún deseo de provocarlos. Por lo demás, tras la desarticulación de Shadow Crew, los rusos se habían retirado del negocio de las tarjetas. O, mejor dicho, se habían dado de baja —de forma más o menos generalizada— de los foros en inglés. El babilónico ir y venir de delincuentes, confidentes, espías y agentes de policía en las webs anglófonas empezaba a ser irritante y opresivo, y aunque ellos no corrieran peligro —en tanto se mantuvieran alejados de los países donde pudiera actuar la ley estadounidense—, el negocio se resentía.

Así pues, los *hackers* rusos crearon una serie de foros exclusiva o mayoritariamente rusófonos, entre ellos Mazafaka.ru. Las fuerzas de seguridad estadounidenses no lo tenían nada fácil para infiltrarse en ellos, y la colaboración con la policía rusa o el influyente KGB se reveló difícil en extremo. La primera línea de defensa de los delincuentes rusos o ucranianos es la jerga local, en cambio permanente. Algunos agentes de policía occidentales podían conversar en ruso, pero tenían muchas dificultades para mantenerse al corriente de los cambios en la lengua relacionados con la cultura popular, que pocos podían seguir desde Washington o Londres.

Mientras las webs rusas seguían operando con toda tranquilidad, en el verano de 2006 Iceman ya había liquidado a casi todos sus oponentes de lengua inglesa. Y cuando averiguaba que alguno de ellos intentaba levantar

cabeza, lanzaba contra él un devastador ataque distribuido de denegación de servicio (DDoS).

Los ataques DDoS se habían convertido en el arma más corriente en el ciberespacio. Eran obra de los llamados *botnets*, el equivalente digital de *La invasión de los ladrones de cuerpos*, la película clásica de Hollywood de los años cincuenta. Un virus «captura» un ordenador, que queda bajo la influencia de lo que se conoce como un servidor de mando y control. El virus infecta de esa misma manera a miles de equipos —a partir de entonces denominados zombis—, convirtiéndolos en esclavos a las órdenes de un todopoderoso servidor de mando y control. A casi todos los efectos, siguen funcionando como ordenadores normales, y los usuarios comunes ni siquiera se percatan de que su máquina ha pasado a engrosar las filas de un vasto ejército de no muertos digitales. Cuando un zombi desarrolla una actividad especialmente intensa, es posible que la inocente víctima perciba una ligera ralentización del equipo, debida por lo común a que su capacidad de trabajo se ve sobrepasada por el envío de miles de millones de correos basura en los que se anuncian alargamientos de pene y vicodina o en los que viajan copias del virus destinadas a infectar nuevos ordenadores.

Pero en ocasiones los *botnets* reciben instrucciones de organizar ataques DDoS, para lo que se requiere que todos los zombis accedan a una determinada página web al mismo tiempo. Las webs o servidores que sufren un DDoS se colapsan ante la imposibilidad de dar cabida a tal cantidad de tráfico de datos y sus páginas se quedan congeladas. Si el ataque es lo bastante potente, el sistema entero se paraliza.

A base de arrogancia y de recurrir cada dos por tres a ataques DDoS, Iceman se ganó la animadversión de buena parte de la comunidad *hacker*. Pero sus tácticas despertaron también la sospecha de que podía estar a sueldo de los federales, ya que muchas de sus víctimas eran *hackers* y delincuentes.

Lo que nadie podía discutirle eran las cifras: Carders Market tenía varios miles de miembros en activo que no dejaban de comprar y vender tarjetas de crédito, cuentas corrientes, virus, identidades y demás. En agosto de 2006, se había convertido en el rey del cibermundo.

Solo tenía una espina clavada. Había una página que se negaba a caer. Cada vez que la atacaba, ya fuera borrando su base de datos y eliminando todos sus archivos, ya ordenando a su ejército de zombis que la hicieran caer de la red, la página aguantaba y, como un tentetieso, volvía a levantarse.

La batalla con Dark Market había empezado.

16

DARK MARKET

El ciberespacio, 2005-2008

El coche trucado descendía por el extremo occidental de los Alpes y el sol se reflejaba sobre las límpidas aguas del Mediterráneo como una confirmación de que aquel había de ser un fin de semana extraordinario. El grupo de veintitantos escandinavos liderado por Recka, el rey de los tarjeteros suecos, salió de la A8 para tomar la carretera de la Grande Corniche, por la que luego bajarían serpenteando a través de las montañas hasta Mónaco.

El principado, uno de los Estados más pequeños y densamente poblados del mundo, pasó buena parte del siglo pasado sumergido en glamur. Gracias al clima de idolatría por las estrellas típico de la posguerra, el país saltó a la fama en 1956, año en que Grace Kelly, una de las figuras más adoradas de Hollywood, ingresó en la realeza al contraer matrimonio con el príncipe Raniero, el heredero al trono monegasco.

Pasados cincuenta años justos de la boda del siglo, un grupo de miembros de Dark Market armados con un peculiar arsenal de plástico planeaba una razia contra aquel templo de la decadencia. Nada más franquear la frontera entre Francia y Mónaco, aparecieron los primeros casinos. Los presupuestos del principado dependen de esas fábricas de billetes desde la década de 1860. Las gentes del país los conocen como «las billeteras de Mónaco», y gracias a ellos los monegascos no pagan impuestos. ¿Para qué? La habitación sencilla en el hotel Monte Carlo Bay, por ejemplo, cuesta ochocientos euros por noche, y, si los huéspedes pueden permitirse pagar ese precio, es evidente que también pueden despilfarrar su estúpido dinero en el casino. El resultado es una sobreabundancia de riquezas generalizada.

Los monegascos nadan, pues, en la abundancia gracias a los multimillonarios que dilapidan sus fortunas en las mesas de *blackjack* o en la ruleta. A muchos visitantes no les importa desprenderse de esas cantidades con tanta ligereza porque se trata de dinero que, en otras circunstancias, habrían tenido que pagar en concepto de impuestos en los países donde ellos o

sus negocios tienen fijada la residencia. Mónaco es un paraíso para la evasión fiscal —y, según la venerable Organización para la Cooperación y el Desarrollo Económico, también para el lavado de capitales—, y las autoridades de este montuoso reducto libre de impuestos no suelen hacer preguntas sobre el origen del dinero de quienes visitan su pequeña patria.

El lugar ideal, pues, para un grupo de piratas armados con doce American Express Centurion, la legendaria Amex negra, una deidad olímpica de la era del plástico que solo concede audiencia mediante invitación especial a los grandes potentados de Occidente, Japón, Hong Kong y Oriente Próximo. En Estados Unidos, los poseedores de la Centurion abonan una cuota de admisión de cinco mil dólares y cuotas anuales de dos mil quinientos. A cambio, obtienen billetes de avión gratuitos, asistentes exclusivos, asesores de compras y afiliaciones a clubes de élite repartidos discretamente por todo el mundo de los que el común de los mortales jamás hemos oído hablar.

¿Y en cuanto al dinero? El dueño de una Centurion no tiene más que enseñarla y dejar que le caigan encima los dólares, euros, libras, francos suizos o yenes de que le hará entrega el empleado de banca de turno con una sonrisa reservada para los clientes de su posición y valía. Casi bastaría una Centurion para pagar el rescate de un rehén capturado por piratas somalíes.

No hay nada extraño en que un grupo de jóvenes con más dinero de la cuenta visiten Montecarlo con el único fin de gastar y gastar a golpe de Centurion; en un ambiente como ese, los jóvenes consentidos son la norma. El objetivo era dejar las doce tarjetas mágicas sacando humo. Primero un hotel de lujo, luego los cócteles y una fastuosa comida, y a continuación el casino. «Fue una fiesta salvaje —recuerda uno de ellos con tono ensoñado—. En 2006, Dark Market empezó a pegar fuerte». Cuando se marcharon, dos días más tarde, los jóvenes habían gastado cuatrocientos mil dólares con sus Amex negras. Incluso ellos mismos admiten que se sorprendieron al ver que era tan fácil. «La gente ni pestañeaba. Nadie puso ningún reparo. Era como si ahí todo el mundo hiciera lo mismo a todas horas».

Los escandinavos no eran los únicos que habían explotado el filón. Maksik, un conocido tarjetero ucraniano, había ganado cientos de miles de dólares vendiendo *dumps* y *fulls* (números de tarjetas de crédito con su PIN y los tres dígitos del reverso de la tarjeta). Cha0, en Turquía, había creado una auténtica factoría criminal mediante la extracción de dinero con tarjetas de crédito clonadas y la venta de clonadoras a todo el mundo para que otros ladrones pudieran robar datos por su cuenta.

Darkmarket.com se fundó en mayo de 2005, pero durante los primeros meses de existencia no consiguió arrancar el vuelo. No fue hasta el otoño de ese año que consiguió atraer a figuras importantes de los foros del sector. El más activo de ellos era JiLsi, el *hacker* de Sri Lanka, creador a su vez de otra web, The Vouched, y moderador en la pequeña pero influyente sección en inglés de Mazafaka.

JiLsi consiguió en poco tiempo ser nombrado moderador global de Dark Market, el escalafón previo al cargo de administrador, y se marcó como meta aumentar el prestigio de la página. Su objetivo era el mismo que el de Iceman con Carders Market: quería que la web fuera reconocida como una de las más importantes del mundo anglófono. Trabajando incansablemente desde la cafetería de internet Java Bean del norte de Londres, logró que en mayo de 2006 el número de miembros hubiera aumentado en varios cientos. En su mayoría eran usuarios de habla inglesa, aunque también había un importante componente de rusos.

Cuando la web empezó a hacerse popular entre los tarjeteros del mundo entero, sus fundadores decidieron cerrarla por miedo a la infiltración de los servicios de seguridad. Uno de ellos temía incluso que Dark Market alcanzase un éxito excesivo. JiLsi y sus amigos, por el contrario, querían seguir sacando partido de su creciente reputación, de modo que registraron la página como darkmarket.ws (el dominio geográfico de Samoa Occidental).

Ahora podían ponerse a trabajar en serio. Además de JiLsi, Dark Market contaba con el patrocinio de un renombrado *hacker* ruso que operaba bajo el nombre de Shtirlitz, un veterano de Carder Planet que ejercía de correa de transmisión entre las webs rusas y Dark Market.

Matrix001 fue otro de los que quisieron echar un vistazo a la página. Su reputación como especialista en diseño gráfico no había hecho más que crecer desde su ingreso en la Asociación Internacional para el Progreso de la Actividad Criminal. Lo que vio lo dejó más bien frío: el panel de mensajes estaba anticuado y la seguridad dejaba bastante que desear. Matrix le envió un mensaje a JiLsi, el administrador, en el que lo informaba sin rodeos de que, debido a las deficiencias del sistema, la web era pirateada a diario por enemigos como Iceman. Matrix se ofrecía a instalar un sistema mejor. JiLsi aceptó encantado y Matrix empezó su ascenso en la jerarquía.

Otros muchos se ofrecieron a colaborar. JiLsi promocionó en poco tiempo a un tal Master Splyntr al cargo de moderador del foro. El nombre de Master Splyntr, alias de un conocido *spammer* polaco llamado Pavel Kaminski, era un guiño inequívocamente adolescente: hacía referencia a la rata que

introduce en las artes marciales a las tortugas *ninja* en la popular serie infantil de dibujos animados. En deferencia a su carisma y habilidad, Master Splyntr también era conocido como «senséi» entre la comunidad *spammer* y *hacker*.

La verdadera identidad de Master Splyntr fue revelada por la organización secreta *antispam* británica Spamhaus.org. Los hombres de negocios, informáticos, exespías y Dios sabe qué más que integran ese grupo mantienen una guerra abierta contra una serie de pesos pesados del mundo del *spam*, el tarjeteo y la pornografía infantil. Su misión consiste en peinar la red en busca de proveedores de servicios de internet perniciosos, es decir, proveedores de servicios de internet que hacen la vista gorda ante las actividades delictivas de sus clientes. Kaminski, según informó en su momento Spamhaus en su página web, era uno de los cinco mayores *spammers* del mundo y el remitente de ingentes cantidades de anuncios no deseados de alargamientos de pene, vicodina y demás.

Que Spamhaus mostrara tanto interés por Master Splyntr significaba que era un hombre marcado; de hecho, cinco cuerpos policiales de distintos países investigaron sus actividades en cuanto se pasó del envío de correo basura al tarjeteo. A Kaminski se lo relacionaba también con la distribución al por mayor de *malware*, virus y troyanos. Era un tipo malo con todas las de ley. JiLsi estaba encantado de haber pescado a un pez gordo como él en las aguas de Dark Market, y, de hecho, mantuvo una estrecha relación tanto con él como con Matrix001. Estaban formando un equipo, y cuando Cha0, el turco, se unió al grupo, Dark Market quedó envuelto en una indudable aureola de éxito.

A simple vista, Dark Market no tenía nada de particular. Su funcionamiento era como el de los paneles de mensajes donde se debate sobre los peligros de ser padre o los placeres de la apicultura. Acceder no era fácil porque los miembros debían presentar una solicitud y someterse a escrutinio, aunque eso casi nunca suponía un problema para alguien familiarizado con el negocio y con un verdadero interés por ingresar en la web. Por razones de seguridad, los negocios en sí —las compraventas— casi nunca se llevaban a cabo en el foro. La página era más bien un punto de encuentro de vendedores y compradores; ahí los fabricantes de máquinas clonadoras entraban en contacto con sus posibles clientes y los dueños de bases de datos de tarjetas reclutaban a las brigadas encargadas de la delicada tarea de ir de cajero en cajero extrayendo el dinero en metálico. Pero los detalles de cada acuerdo casi siempre se discutían en conversaciones privadas a través de redes ICQ encriptadas. Una vez pactado un acuerdo, las partes volvían a la web para

acogerse al servicio de fideicomiso, mediante el cual los administradores garantizaban el cumplimiento del trato.

El foro atraía cada día a más adeptos y el negocio iba viento en popa. Determinados miembros actuaban como puente entre los delincuentes rusos y los tarjeteros occidentales. La influencia geográfica de la página era cada vez mayor. Turquía empezaba a convertirse en un territorio importante, y las comunidades de España y Alemania crecían a buen ritmo, en tanto que los tarjeteros galos —que, como la mayoría de los franceses, se sentían más cómodos en entornos francófonos también en la red— intentaban engrasar su inglés para no perder el tren.

La edad de oro de Dark Market estaba a punto de comenzar.

17

LA OFICINA

La oficina de Renu Subramaniam era uno de los terminales del Java Bean. Durante los últimos dieciocho meses, Renu había tenido que trabajar soportando un estrépito continuo, ya que la cafetería quedaba delante del estadio de Wembley, por entonces inmerso en un proceso de remodelación total que, a mediados de 2006, ya había superado tanto los plazos como el presupuesto.

A primer golpe de vista, la cafetería era como cualquier otra de las miles que hay diseminadas por el globo. La ubicación del local, entre el bar Bowling Nail y una gestoría de aspecto lúgubre, no era la ideal. En él había varias pantallas viejas y en mal estado y teclados grasientos conectados a ordenadores poco fiables con las etiquetas de marca falsas típicas de las imitaciones baratas de Asia oriental. Solo Dios sabe qué clase de actividades tenían lugar en el interior de las destartaladas mamparas de madera que separaban aquellas mugrientas consolas.

Inclinados sobre las pantallas podían encontrarse adolescentes que pasaban las horas jugando en línea, a menudo en estados de concentración inauditos; mochileros que redactaban simpáticos correos con sus impresiones sobre las tierras recién descubiertas; chiquillos curiosos y hombres de mediana edad frustrados que navegaban por extravagantes webs pornográficas; jóvenes idealistas que planificaban protestas con la confianza de que el anonimato de la red los ayudase a burlar al Gran Hermano; traficantes de drogas que discutían puntos de entrega y métodos para lavar dinero, y ciberdelincuentes que se conectaban para ver a cuánto ascendía su última estafa.

Aparte de su ubicación, a la sombra del nuevo estadio de Wembley, el Java Bean también era peculiar por otro motivo. Generalmente, los ordenadores de las cafeterías de internet están protegidos solo de forma parcial frente a ataques externos. Virus, troyanos y demás bacterias digitales campan por ellos a su antojo, como sus equivalentes orgánicos en los hospitales con medidas de higiene deficientes.

Renu, sin embargo, se tomaba la seguridad muy en serio y había convencido al encargado del Java Bean de que instalase en los sistemas de la cafetería un programa especial llamado Deep Freeze. La aplicación restauraba en los discos duros una configuración predeterminada, de modo que la red no «detectara» ningún tipo de *malware* descargado a lo largo del día. Así, los programas maliciosos quedaban sin efecto y Renu reforzaba su protección.

Si el Java Bean era la oficina de Renu, el fichero donde se acumulaban los secretos de Dark Market consistía en un pequeño lápiz de memoria. Renu siempre llevaba su memoria portátil literalmente pegada al corazón. Cuando llegaba a la oficina, insertaba el dispositivo en uno de los terminales y se ponía a trabajar en Dark Market.

Una vez conectado, Renu se ponía la máscara de pirata y se transformaba en JiLsi, uno de los ocho administradores que dirigieron Dark Market a lo largo de sus tres años de existencia. El equipo, que en ningún momento estuvo formado por más de cuatro miembros, se convirtió en una de las unidades más influyentes del panorama tarjetero global. El hecho de ocupar un cargo prominente no se traducía en ingresos adicionales, pero era un puesto privilegiado que inspiraba un respeto considerable entre la comunidad de *hackers* y *crackers*. Los administradores, además, disponían de acceso a grandes cantidades de información y gozaban de poder virtual de vida o muerte: en su mano estaba excluir a determinados miembros con motivo de transgresiones reales o presuntas.

El codiciado cargo de administrador tenía dos grandes inconvenientes. En primer lugar, implicaba mucho trabajo, unas quince o diecisiete horas diarias de tecleo constante y sin posibilidad de vacaciones, ya que debían estar disponibles todos los días del año. Master Splyntr, por ejemplo, siempre llevaba encima un teléfono móvil que lo alertaba cuando alguno de los miembros requería su ayuda. JiLsi se quejaba de que se conectaba a las nueve de la mañana y a las diez de la noche seguía sentado delante de la pantalla. La mayor parte del trabajo era puro trámite: examinar los mensajes para asegurarse de que los miembros cumpliesen las reglas del foro y colgasen los mensajes en la sección adecuada. Casi todo el tiempo se perdía en burocracia, en detalles triviales y soporíferos.

En segundo lugar, el equipo de administradores estaba conectado de forma permanente a los sistemas de las webs. Su impronta digital era, *a priori*, mucho más visible que la de los miembros ordinarios, lo que los convertía en un objetivo de primer orden para los ciberpolicías.

La situación resulta paradójica si tenemos en cuenta que generalmente eran los miembros «ordinarios» quienes ganaban más dinero en Dark Market: los administradores asumían los mayores riesgos a cambio de una recompensa económica mínima. A lo largo de esos tres años, JiLsi y Matrix ganaron una miseria, y Master Splyntr solo cobraba por mantener los servidores, el resto de sus ganancias provenían de los envíos de correo basura.

Mención aparte merece Shtirlitz, personaje enigmático presente desde el primer momento. Su alias hace referencia al personaje de ficción Max Otto von Stirlitz, que en las novelas de Yulian Semiónov es un alto oficial nazi que trabaja como espía para Moscú durante la segunda guerra mundial. Conocido como el James Bond ruso, Stirlitz arraigó en la mentalidad rusa en la década de 1970 gracias a una serie de populares películas basadas en los libros. Stirlitz, tipo discreto y bien parecido, sigue siendo un poderoso símbolo patriótico en la Rusia poscomunista gracias a su gran valor, inteligencia e incondicional compromiso patriótico.

Hasta aquí Stirlitz, el espía soviético. Pero ¿quién era Shtirlitz (que transliteraba su nombre del ruso, de aquí la adición de la hache), el tarjetero? ¿Era también él un agente del KGB? ¿O quizá un agente doble, a sueldo de los federales o del Servicio Secreto? ¿Acaso un maestro de tarjeteros? Uno de los miembros de Carder Planet que lo conoció lo describe como un «tipo de aspecto ario, al borde de la treintena». Poseía varios pasaportes falsos y, durante una época, residió en Praga. En Carder Planet se hablaba de él como de «una persona buena y de fiar», pero con el tiempo los tarjeteros empezaron a sospechar que quizá su verdadero vínculo con el personaje de ficción consistía en ser uno de los más experimentados agentes de la ley estadounidenses.

Fueran cuales fueran sus motivos para convertirse en uno de los principales miembros de Dark Market, su presencia era constante aunque silenciosa, y su participación, más bien escasa. Más tarde aparecería otro administrador, Lord Cyric, que, igual que él, parecía no comprar ni vender nada. Ambos estaban demasiado ocupados manteniendo el barco a flote y labrándose una reputación de proporciones legendarias entre sus cofrades.

Al mismo tiempo, los dos tenían secretos. A veces las cosas no son lo que parecen.

Resulta irónico que quien más se preocupara por preservar su seguridad personal fuese, en muchos respectos, el más transparente. Hablamos de Cha0, el delincuente turco, cuya aparición en los foros fue relativamente tardía. A diferencia de los demás, Cha0 no era un veterano de Shadow Crew ni de la

IAACA, sino que surgió como de la nada a principios de 2006 en calidad de propietario de un foro llamado Crimeenforcers.com, una web de diseño elegante que ofrecía toda clase de ayudas a los aspirantes a ciberdelincuentes. La página destacaba sobre todo por sus tutoriales en los que un dibujo animado que representaba a Cha0 guiaba a los usuarios a través de los vericuetos del mundo tarjetil.

Cha0 se servía de Dark Market para promocionar Crime Enforcers (la publicidad de pago representaba para los foros una importante vía de ingresos), y su presencia ubicua, así como sus incesantes transacciones, pronto se tradujeron en una verdadera influencia. Ingresó en Dark Market en febrero de 2006, y al cabo de siete meses era uno de sus cabecillas.

A diferencia de sus colegas, Cha0 era uno de esos pocos casos en que la vocación delictiva se conjuga con una mente brillante. Su motivación para aceptar el cargo fue muy simple: podía serle útil con vistas a ampliar su negocio como distribuidor de accesorios para perpetrar delitos económicos, tales como las clonadoras, los dispositivos de lectura, almacenamiento y transmisión de datos de las tarjetas de crédito de las víctimas.

Mas, como ocurre con otras figuras destacadas de Dark Market, la historia de Cha0 resultó ser bastante más bizantina, y aquí el adjetivo viene como anillo al dedo, por tratarse de un residente de Estambul.

Dejando aparte el anómalo caso de Cha0, los ladrones más exitosos de Dark Market no participaban en el mantenimiento de la página. Eran gente como Freddybb y Recka, los tarjeteros de Scunthorpe y Suecia, que, si entraban, era para liquidar algún negocio, y luego desaparecían durante días, semanas e incluso meses. De aquí que los ciberoperativos de los cuerpos policiales de los distintos países hayan resultado en la detención de un mayor porcentaje de *geeks* que de delincuentes puros y duros.

La abnegada labor de los cuatro administradores giraba en torno a cuatro tareas principales. La protección de los servidores de la web y su mantenimiento general eran responsabilidad de Master Splyntr y Matrix001. La mayor parte de las amenazas que llegaban a la página no provenían de los cuerpos policiales, sino de los rivales y enemigos que Dark Market tenía repartidos por todo el ciberespacio criminal, como Iceman. Splyntr, Matrix y JiLsi suspiraban resignados cada vez que surgía una pelea entre miembros. El proceso solía ser siempre el mismo, tanto era así que, a su pesar, Splyntr terminó por acostumbrarse: un tarjetero acusaba a otro de haber infringido alguna norma, a veces sin base, a veces con razón. Acto seguido, el acusado armaba una pataleta, y, al poco tiempo, organizaba un *botnet* para lanzar un

ataque DDoS. Entonces, miles de ordenadores bajo un único equipo de mando y control solicitaban acceso a Dark Market, provocando la caída de la página. En el mundo real, se decía Splyntr, la solución habría sido ir a por el causante y molerlo a palos, pero en el ciberespacio no queda más remedio que cerrar la web y esperar a que el atacante se calme o negociar algún tipo de acuerdo.

Los administradores, por lo tanto, estaban obligados a tener los ojos puestos en los conflictos que se gestaban entre los miembros e intentar contenerlos antes de que estallasen. Por regla general, los ciberdelincuentes tienen los modales de un chimpancé y la lengua de una verdulera siciliana. El anonimato de la red fomenta una desconfianza intrínseca, sobre todo en el mundo del hampa, siempre bajo la amenaza de la policía y la supuesta invulnerabilidad que el usuario cree que le confiere el anonimato. En foros como Dark Market, los insultos desembocaban a menudo en una guerra verbal abierta, y esa era una de las mejores bazas de la policía; cuando una comunidad vive dividida por las suspicacias, cualquiera con un mínimo de habilidad puede manipular las disputas en provecho propio.

El equipo de administración era el que decidía el lugar de los miembros dentro de la jerarquía de Dark Market. Los cuatro se reunían en privado —en un foro al que solo ellos tenían acceso— y discutían, por ejemplo, si tal vendedor de tarjetas de crédito robadas tenía un historial lo bastante fiable como para merecer el anhelado título de «vendedor cualificado», lo que le permitiría vender tarjetas sin restricciones a través de Dark Market.

Los administradores eran asimismo los encargados de investigar la presencia de ciberpolicías, por no hablar de los «puercos y *rippers*», los delincuentes que se negaban a acatar las reglas del submundo.

La detección de *rippers* también era un factor clave en la tercera y más importante función de los administradores: gestionar el servicio de fideicomiso a fin de asegurar que los reyes del juego sucio jugasen limpio entre ellos. Como en el caso de la primera web del sector, Carder Planet, la correcta gestión de los fideicomisos se reveló crucial a la hora de convertir a Dark Market en la principal web criminal del momento. El servicio estaba a cargo de JiLsi, pero las decisiones importantes las tomaba Cha0.

Por último, los administradores debían mantenerse ojo avizor para evitar que nadie utilizase la web para distribuir pornografía infantil o dedicarse a la compraventa de drogas y armas. No lo hacían movidos por una repulsa moral, sino por el convencimiento de que, si se limitaban al tráfico de tarjetas y datos personales, la policía mostraría menos celo en sus actuaciones contra la web.

Para Renu, la primera mitad de 2006 fue muy movida. La mala suerte empezó en febrero. Salió del Java Bean tras una dura jornada de trabajo y se dispuso a pasar la noche abrazado al Martell y su pipa de crac. A la mañana siguiente, al levantarse, vio que su valioso lápiz de memoria no se hallaba en el lugar habitual, guardado cerca de su pecho. ¡Se había olvidado el chisme de las narices en la cafetería!

El pánico se apoderó de él. Cuando llegó al Java Bean, fue directo al encargado para preguntar si alguien lo había encontrado. El encargado negó con la cabeza. «¡Por tu culpa acabo de perder un cuarto de millón de libras!», gritó Renu, olvidando por un momento que el único responsable de aquel desastre era él. Le preocupaban menos sus limitados fondos que el dinero y los datos que tenía en fideicomiso.

A lo largo de las semanas siguientes, JiLsi emprendió una operación de control de daños. Debía garantizarles a los miembros de Dark Market que habían depositado su confianza en él que no corrían peligro. Al mismo tiempo, en el mundo real, Renu se las veía y se las deseaba para pagar las hipotecas sobre una serie de cuchitriles que había adquirido en la zona norte de Londres. Dark Market prosperaba, pero no podía decirse lo mismo de JiLsi. Al contrario, las deudas no dejaban de acosarlo y tuvo que pedir prestado a algunos «amigos». El hecho de ser un fugitivo del ciberespacio no suponía ninguna ventaja a la hora de abrirse camino en el «submundo» tradicional.

A pesar de la pérdida del lápiz de memoria, Renu siguió entregado en cuerpo y alma a Dark Market. Sin embargo, el estrés que le provocaba la dirección de la página empezaba a hacérsele insoportable, sobre todo porque veía que Dark Market y Carders Market se hallaban enfrascados en una lucha a muerte. La web era vulnerable, pero JiLsi lo era todavía más, y a veces tenía la impresión de que la situación terminaría superándolo.

Iceman recrudeció sus ataques mediante el envío de DDoS y arrojando contra Dark Market todas las armas digitales que caían en sus manos. Los tarjeteros de todo el mundo se alinearon con una u otra de las páginas. Argüían que era el oponente quien debía ceder y dejar el sector en manos de una única megaweb. De hecho, ese era el principal argumento de Iceman: que en ese campo la competencia no redundaba en una mayor eficacia, sino solo en rencor.

En septiembre de 2006, los ataques no habían cesado y Renu se hallaba al borde de la desesperación. Además, su dependencia del crac era cada vez

mayor, lo cual suponía un peligro para su seguridad —por no decir para su salud—, así como para la de Dark Market.

Finalmente, decidió hablar de los ataques contra Dark Market con Master Splyntr, a la sazón moderador, es decir, dos escalafones por debajo de JiLsi, que era el administrador principal. Master Splyntr (Kaminski) llevaba tiempo diciendo que JiLsi debía cederle el control de los servidores. Kaminski aseguraba que sus dispositivos de seguridad eran mejores y que, si delegaba en él, JiLsi se quitaría mucha presión de encima.

Master Splyntr figuraba en el último puesto de la lista de preferencias de JiLsi. Antes que a él, Renu le había ofrecido el cargo a Cha0, pero el turco se había negado a aceptarlo, sin duda porque no estaba dispuesto a desempeñar tan ingrata tarea. Nadie más parecía dispuesto a comprometerse, de modo que JiLsi no tuvo más remedio que proponérselo a Master Splyntr.

Kaminski recibió el aviso hacia las once y media de la noche a principios de octubre de 2006. «Mis servidores están listos, JiLsi», contestó. Feliz de no tener que volver a responder de la vulnerabilidad de sus servidores, JiLsi dejó a un lado sus dudas: «Muy bien. ¡Adelante!».

Tal vez porque temía su irritación, JiLsi no consultó la decisión de ceder el control del servidor a Master Splyntr con el resto de los administradores, aunque, una vez efectuado, nadie pareció oponerse. Splyntr no tardó en mostrarse más eficaz que JiLsi, y todo el mundo quedó convencido de que era la persona idónea.

Kaminski cumplió lo prometido: sus servidores eran efectivos y seguros. No solo eso, sino que cada vez que alguien (*hackers*, policías, servicios militares o de inteligencia) intentaba averiguar cuál era la localización real de Dark Market, el intruso se veía incapaz de ir más allá de un servidor anónimo situado en Singapur.

Master Splyntr fue nombrado administrador. El tráfico de la página volvió a aumentar. Cada vez que Iceman atacaba la web y destruía su base de datos, Master Splyntr la restauraba en menos de veinticuatro horas. Iceman era sin duda alguna el mejor en el apartado técnico, pero con su arrogancia se había ganado la antipatía de cientos de tarjeteros. Dark Market ganó fuerza y parecía que nada podía evitar su ascenso a la cumbre. Pero Iceman todavía no había jugado su última carta.

18

MENTES SUSPICACES

Bajo una calma aparente, Iceman escondía una furia demoledora. Había perdido la cuenta de la hora. Podían ser tanto las tres de la madrugada como las tres de la tarde; la preparación de un ataque de grandes proporciones requiere invertir horas, y es fácil desorientarse. Para los *hackers* más obsesivos, las nociones de espacio y tiempo se evaporan. Cuando lo invadía la furia, Iceman perdía el mundo de vista; lo único que le importaba era la llamada de Némesis, la diosa de la venganza.

La diosa se manifestaba bajo distintas apariencias. En primer lugar, bajo el nombre de El Mariachi, un rencoroso tarjetero cuya web, The Grifters, Iceman había destruido. Desde su promontorio digital, El Mariachi afirmaba poseer pruebas irrefutables de que Iceman era un colaborador del FBI. Sus acusaciones contaban con el respaldo de Lord Cyric, el perrito faldero de El Mariachi, cuyos ladridos eran audibles en todos los foros. Como tantos otros, Iceman sentía un gran desprecio por Lord Cyric.

Unos y otros cruzaban envenenadas acusaciones por las distintas webs. Era como una guerra entre clanes mafiosos, con la diferencia de que nadie sabía con certeza a qué familia pertenecía cada uno, ni quién podía ser un confidente o un federal. Era el caos.

Hasta que un día Iceman descubrió una información que en ese momento consideró veraz y que lo dejó poco menos que anonadado en su cómodo apartamento del centro de San Francisco, pagado por Jeffrey Normington y otro socio a cambio del suministro regular de números de tarjetas de crédito robadas. Desde ahí, entre bordes de *pizza* resecos y latas de cola, Iceman administraba Carders Market y atacaba sin tregua otras páginas. En octubre, había logrado piratear con éxito el núcleo de los servidores de Dark Market.

Mientras examinaba el tráfico de los administradores, identificó de pronto unas direcciones IP de aspecto sospechoso. Cualquiera puede buscar una dirección IP y comprobar su ubicación, qué persona física o jurídica está asociada a ella, así como el nombre de su proveedor de servicios de internet. Una de la direcciones estaba registrada a nombre de una compañía llamada

Pembrooke Associates. Iceman puso la red patas arriba en busca de información, pero no halló nada excepto una web con un listado de empresas. En él figuraba el nombre y un número de teléfono. Acto seguido, realizó una búsqueda inversa en el listín telefónico y dio con la dirección física: 2000 Technology Drive, Pittsburgh (Pensilvania).

Al leer la dirección, ni siquiera un tipo como Iceman pudo reprimir un escalofrío. A decir verdad, ya se había cruzado con ella un par de semanas antes, después de que uno de sus colegas de Carders Market hubiera encontrado en una web una plantilla con el acrónimo NCFTA y esa misma dirección de Pittsburgh. Cuando Iceman buscó la organización, descubrió que se trataba de la Alianza Nacional para la Formación en Informática Forense, un organismo semigubernamental que colaboraba con varias agencias de seguridad estadounidenses en todo tipo de asuntos relacionados con la seguridad electrónica.

Desde su escondite en las catacumbas virtuales, de repente Iceman sintió la gélida mano del mundo real. Siempre había sospechado que le ley acechaba detrás de cada esquina, pero aquello no dejaba lugar a dudas; estaba seguro de que no podía tratarse de un error. Tras tantos meses convencido de ser intocable y de tener en sus manos a la comunidad tarjetera, Max Vision empezó a preocuparse.

Tras una larga serie de consultas, tres de los colegas de Iceman en Carders Market —silo, c0rrupted0ne y dystopia— decidieron contactar con Matrix001, de Dark Market, para compartir con él su preocupación acerca de aquella dirección IP y el FBI, y para trazar un plan a seguir. Matrix001 era el único administrador al que nadie creía vinculado con ningún cuerpo de seguridad, de modo que le enviaron un escueto mensaje por ICQ con las pruebas relativas a la NCFTA y la dirección de Technology Drive en Pittsburgh:

> *dystopia*: Hace tiempo que lo sabemos, pero al fin tenemos pruebas.
> *dystopia*: Matrix, DM es una tapadera.
> dystopia: 100 %.
> *c0rrupted0*: Nos hemos esforzado por hacer las paces, y si sacamos esto a la luz la policía vendrá DIRECTAMENTE a por nosotros, pero si no decimos nada seremos responsables de toda la gente a la que jodan.
> *siloadmin*: ¡Feliz día, administras una web tapadera!

siloadmin: Pembrooke Associates 2000 Technology Dr. Pittsburgh, Pensilvania, 15219. ¿Te suena 2000 Technology Dr.?

Matrix temía que ahí hubiera gato encerrado. Por norma no se fiaba de nadie, y mucho menos de c0rrupted0ne y silo. Durante mucho tiempo, Carders Market no había escatimado recursos para acosar a Dark Market con el fin de destruirla por todos los medios posibles. Examinó el documento y, pese a no ser el inglés su lengua nativa, enseguida vio que estaba trufado de errores:

Matrix001: El documento de Word es falso.
Matrix001: ¿Ninguno de vosotros se ha fijado en las erratas?
Matrix001: Ah, y en el encabezamiento no figura ninguna empresa ni nombre de ningún tipo…
Matrix001: … donde ponga NCFTA.
Matrix001: Solo la dirección.
Matrix001: Ah, y por poner solo un ejemplo: se escribe *disponible* no *disponibile*.
Matrix001: ¿Queréis que siga?

Siloadmin contestó poniéndose a la defensiva, como si estuviera molesto consigo mismo por no haber reparado en las erratas:

siloadmin: Escucha, Matrix:
siloadmin: Ya sé que el puto documento parece falso, erratas, etc.
siloadmin: Pero es lo que hay.
siloadmin: Yo no me he sacado esta mierda de la manga.
Matrix001: Ninguna empresa del mundo redactaría un documento como ese.
Matrix001: Es totalmente ridículo.

Todo aquello podía muy bien ser una emboscada y, según Matrix, la conversación no hacía más que confirmarlo. Acusar a los foros rivales de formar parte de operaciones encubiertas de la policía era una táctica habitual destinada a asustar a los miembros para que se pasasen a la competencia. Matrix estaba convencido de que, si los adeptos de Dark Market desertaban, Iceman y Carders Market los reclutarían de inmediato, y eso podía poner en peligro la existencia misma de Dark Market.

Además, silo, dystopia y c0rrupted0ne habían insistido —quizá demasiado— en que Matrix abriera otro archivo, comprimido con zip, conocido como rar. Los archivos zip son la principal fuente de transmisión de troyanos, y Matrix estaba seguro de que ese había sido diseñado por el equipo de Carders Market para aspirar todos los secretos de Dark Market de su ordenador. Empezó a preguntarse si Iceman y sus adláteres no estarían en la fase dos de un plan audaz trazado por el FBI para acabar con Dark Market.

Eran ya las nueve y cuarto de una glacial mañana de noviembre en el centro de Alemania, pero Matrix sabía que debía actuar con celeridad. Sin perder un instante, se puso en contacto con el resto de los administradores de Dark Market y les avisó de que Iceman y sus lacayos estaban a punto de denunciar a la web:

> *Matrix001*: He dicho que mi rar no funciona, así que no he descargado el archivo ni lo he abierto.
> *Matrix001*: Apuesto a que es un troyano.
> *Matrix001*: Y si echáis un vistazo a la info que me han pasado, parece falsa…
> *Matrix001*: Pero leedla vosotros mismos…

19

DONNIE BRASCO

Pittsburgh, octubre de 2006

El agente especial Keith J. Mularski, de la División Cibernética del FBI, estaba consternado, y no solo porque los Steelers estuvieran haciendo una temporada mediocre después de su sensacional victoria en la Super Bowl. Como abonado al Heinz Field, el estadio de los Steelers, Mularski siempre había tenido muy claro que el fútbol americano no es un asunto de vida o muerte, sino mucho más que eso. Por una vez, sin embargo, tenía problemas mucho más serios.

Cual Donnie Brasco virtual, Mularski llevaba varios meses sumergido en el creciente mar de delincuencia de la red. Por supuesto, su vida no había corrido el mismo riesgo que la del agente Joe Pistone al hacerse pasar por Brasco para adentrarse en la guarida de las mafias más peligrosas de Nueva York. Pero Mularski se las había visto y deseado para conseguir que sus superiores dieran luz verde a una operación sin precedentes destinada a infiltrarse en el ciberespacio. Su coste era elevado y entrañaba el peligro de una denuncia por incitación al delito. Por ello los agentes del FBI sometían a escrutinio todos y cada uno de sus movimientos para evitar deslices. Lo que había ocurrido, sin embargo, no había sido un desliz. Había sido una colisión frontal.

El momento no podía ser menos oportuno. Mularski había realizado grandes avances sin levantar sospechas. Estaba a punto de obtener la colaboración de varios cuerpos de seguridad extranjeros para su plan a largo plazo de lanzar una espectacular serie de redadas en todo el mundo. Había creado un personaje con nombre y pasado, y había conseguido que, en un espacio de tiempo notablemente corto, muchos ciberdelincuentes dieran crédito a sus mentiras. Mularski se había ganado la confianza de muchos de sus objetivos.

Y ahora, por culpa de la incuria de un colega que había dejado un archivo con el membrete de la Alianza Nacional para la Formación Ciberforense en

un ordenador, corría el peligro de ser descubierto y de que aquella operación tan intrincada terminase en un fiasco.

Era la primera incursión del FBI en el campo de la delincuencia informática. Hasta entonces, las investigaciones en ese ámbito habían corrido a cargo del Servicio de Inspección Postal estadounidense y, sobre todo, del Servicio Secreto. En 2004, ya no cabía duda de que la delincuencia informática era uno de los sectores con mayor crecimiento dentro del crimen organizado. Cada día eran más las entidades y personas víctimas de la actividad de los piratas. El de las tarjetas de crédito era el problema más grave debido a la gran cantidad de robos y usos fraudulentos. Pero también se daban casos de espionaje industrial en los que los secretos comerciales de grandes compañías eran robados y vendidos a la competencia por parte de los mismos *hackers* involucrados en el fraude de tarjetas. La misma Cisco Systems había visto cómo un competidor chino robaba y copiaba los planes de su servidor más avanzado, lo que demostraba que ni siquiera las empresas supuestamente más seguras estaban a salvo.

La falta de coherencia en materia de seguridad informática, tanto en el ámbito gubernamental como en el privado, empezaba a preocupar a la Casa Blanca, al Congreso y al Pentágono. La mayoría de los organismos y ministerios ignoraban su vulnerabilidad o se sentían tan impotentes frente al gran número de ataques dirigidos contra ellos que preferían esconder la cabeza en el suelo a la espera de que el problema desapareciera por sí solo.

Quien no podía permitirse eso era el Pentágono, que todavía intentaba recuperarse de la «Lluvia de Titanio», una serie de ataques dirigidos contra los sistemas informáticos del Departamento de Defensa con origen en China destinados a obtener documentos secretos almacenados en archivos mal protegidos.

Los grandes bancos todavía estaban tambaleándose de resultas de la llamada vulnerabilidad del valor de verificación del PIN, con la que Citibank y Bank of America habían perdido decenas de millones de dólares en efectivo en tiempos de Shadow Crew. Aunque el problema había sido resuelto, cientos de bancos seguían regalando dinero a los tarjeteros a través de los cajeros automáticos.

En una palabra: caos.

No era difícil imaginar las consecuencias. En breve, una gran porción del dinero de los contribuyentes empezaría a destinarse a los problemas de la delincuencia informática, el ciberespionaje industrial y la guerra informática, y ningún cuerpo de seguridad querría renunciar a su parte del pastel. Al FBI le

parecía excesivo que el Servicio Secreto se adjudicase tres cuartas partes de aquel suculento presupuesto por haberse colgado la medalla del desmantelamiento de Shadow Crew, razón por la que reclamaba su primacía en ese campo aún incipiente.

El FBI, el mayor y más potente de los organismos de seguridad de Estados Unidos, se oponía a ello. Su director, Robert Mueller, deseaba introducirse en el terreno virtual para hacerse con los fondos, pero también porque su intención era remodelar el FBI para convertirlo en algo más que un cuerpo policial: en una agencia de inteligencia de ámbito nacional. El plan de Mularski no solo consistía en atrapar delincuentes, sino también en recabar información. Ese cambio de orientación en la cúpula ayudó a rebatir las objeciones de algunos de los funcionarios más veteranos, y Mularski, que no había escatimado medios para resaltar la importancia de su operación encubierta, obtuvo la autorización. El descubrimiento de Iceman, por lo tanto, no solo ponía la operación Dark Market al borde del precipicio; también estaban en juego la financiación del FBI y su capacidad para llevar a cabo operaciones informáticas. Sobre los hombros de Mularski pesaba una responsabilidad abrumadora.

Su primera reacción fue de desesperanza. La partida había terminado, pensó, y su equipo, que tan duro había trabajado, tendría que humillarse y rendir cuentas a sus superiores, algunos de los cuales responderían diciendo: «¡Os lo habíamos advertido!». Pero una de las razones por las que el FBI había puesto a Mularski al frente de su programa de formación era su capacidad de reacción frente a la adversidad. Pasado el susto, decidió que no arrojaría la toalla sin presentar batalla.

El destino de la familia Mularski había corrido paralelo al de Pittsburgh en el siglo XX. Su tatarabuelo se había embarcado en Hamburgo en 1892 y había llegado a Baltimore con solo un dólar en el bolsillo. Keith era un estadounidense de pura cepa, pero el sustrato étnico de muchas de las comunidades europeas de la ciudad —polaco, en el caso de Mularski— sigue teniendo un gran peso.

Repartidas entre las modestas casas de madera, los cines *art déco* y las salas de baile del hoy en día pintoresco South Side de Pittsburgh, se encuentran varias iglesias y centros culturales de las muchas comunidades eslavas —checa, polaca, serbia, eslovaca, ucraniana y otras— que confluyeron en esa ciudad estratégicamente situada en el oeste de Pensilvania. A principios del siglo XX, Andrij y Julia Warhola, una pareja de primos rutenos procedentes del rural noreste de Eslovaquia, emigraron a Pittsburgh,

donde se desprendieron de la *a* final del apellido y dieron a luz a una de las figuras más influyentes del arte del pasado siglo.

Los robustos puentes de acero y las placas de la Norfolk and Western Railway recuerdan la decisiva contribución de Pittsburgh al predomino económico global de Estados Unidos en el siglo XX. Con el acero de sus industrias se fabricaban acorazados, aviones, automóviles y plantas industriales que se extendieron por el mundo entero. Sin embargo, han pasado varias décadas desde los tiempos en que las negras nubes provenientes de aquella hidra productora de acero envolvían la ciudad en las tinieblas, arrojando las partículas contaminantes que le valieron a Pittsburgh el número uno en enfermedades pulmonares del país.

El esmog ya no nubla la ciudad y Pittsburgh se considera uno de los mejores lugares para vivir de todo Estados Unidos. El sol reluce y, tras quince años de pobreza y decadencia, en la década de 1990 la ciudad se reinventó como uno de los centros de producción de alta tecnología de la Costa Este.

Mularski fue uno de los que dejaron la ciudad en los años ochenta, tras licenciarse en historia en la Universidad Duquesne. Por entonces, el lugar era un erial. Su padre podría haber sido la reencarnación de Willy Loman. Mularski padre fue uno de los primeros en acusar el revés en la fortuna del gigante, perdió su trabajo como viajante en los años setenta y nunca llegó a recolocarse. A partir de entonces, la familia malvivió con las ganancias de la madre de Keith, ayudante ejecutiva.

La población de Pittsburgh se había reducido en un tercio durante la vida del joven Keith. El muchacho no estaba dispuesto a ver cómo la ciudad seguía declinando, de modo que se mudó a Washington con su esposa. Tras conseguir empleo en una gran empresa de muebles con servicio en todo el país, Mularski pudo demostrar sus habilidades en los campos de gestión y ventas. A primera vista, el trabajo como encargado de ventas parece no guardar relación alguna con la delincuencia informática, pero las técnicas aprendidas en la empresa fueron la base de su trabajo como ciberpolicía en el FBI.

La «ingeniería social» —el arte de persuadir a las personas para que hagan cosas que a todas luces obran en contra de sus intereses— es el fundamento de la delincuencia informática. ¿Cómo, se pregunta el timador, puedo convencer a mi víctima para que me entregue su contraseña? ¿Cómo conseguir que abra un correo electrónico con un troyano oculto en el código? ¿Cómo hacer que encienda el ordenador?

El ciberladrón tiene varias posibilidades obvias. Los dos métodos infalibles son las descargas de música y la pornografía. El sexo es uno de los incentivos más potentes; por fuerza, ya que en términos evolutivos encontrar pareja suele ser misión de alto riesgo. Las personas estamos dispuestas a afrontar peligros para satisfacer nuestros deseos sexuales, y los fabricantes de virus informáticos fueron los primeros en entenderlo. La promesa de un par de pechos suele ser suficiente para lograr que el usuario incauto pulse un hipervínculo que descargará un programa destructivo en su equipo. Si tiene suerte, será redirigido a la fotografía deseada, aunque eso rara vez compensa haber revelado los secretos de su ordenador a un pirata remoto y sin rostro. No por azar uno de los virus de mayor éxito se propagó mediante un correo electrónico cuyo asunto rezaba: «*I Love You*».

Si bien los encargados de ventas no suelen esparcir virus, ellos, como los ciberladrones, son consumados ingenieros del alma humana. Su trabajo consiste en convencer a sus potenciales clientes para que inviertan en artículos que no desean o no necesitan. «Vender lo que tienes a alguien que lo desea no es hacer negocio —sentenció en cierta ocasión el capo mafioso Meyer Lansky—. El negocio es vender lo que no tienes a alguien que no lo desea». Como mínimo, los encargados de ventas saben persuadir a sus clientes para que compren los artículos más caros. De modo que, cuando el novato agente Keith Mularski fue aceptado en la recién creada División Cibernética del FBI, tenía una gran ventaja de su parte: sabía cómo ganarse a la gente, cómo engañarla, comprenderla, exhortarla, persuadirla, atraerla. Para ser policía, era un maleante de lo más convincente.

En el año 2000, Pittsburgh había cambiado. La ciudad siempre había sido depositaria de grandes donaciones filantrópicas. Por todas partes eran visibles las huellas de Carnegie, Heinz y Mellon, los colosos de la oleada industrial de finales del siglo XIX y principios del siglo XX. Tras el desplome industrial, la ciudad, en parte, se había reinventado gracias a la inversión en informática y tecnología de la Universidad Carnegie Mellon, considerada como una de las veinte mejores instituciones de enseñanza superior del mundo.

Fundada por el prominente industrial de origen escocés Andrew Carnegie, la universidad empezó su andadura como escuela técnica y, en 1967, se fusionó con el Mellon Institute of Industrial Research. Durante los difíciles años ochenta y principios de los años noventa, la Universidad Carnegie Mellon estudió el ocaso de Pittsburgh y pensó cómo contrarrestarlo. La universidad era famosa por su labor en el campo de la seguridad informática. Junto con el Massachusetts Institute of Technology y Silicon Valley,

Pittsburgh emergió como una de las mecas informáticas de Estados Unidos, con grandes especialistas en asuntos de seguridad.

La presencia de la universidad explica en buena medida la conformación de la nueva Pittsburgh, incluida la aparición en 1997 de la Alianza Nacional para la Formación Ciberforense, una organización sin ánimo de lucro financiada por bancos y varias corporaciones cuyo objetivo era tender puentes entre la docencia, el sector privado, las fuerzas de seguridad y las agencias de inteligencia como reacción a la creciente inseguridad en la red. Esa fue la razón por la que, con el nuevo milenio, Keith Mularski regresó a su ciudad natal para trabajar en las discretas oficinas acristaladas del número 2000 de Technology Drive.

Miró por su ventana del cuarto piso y pensó que él era prácticamente el responsable único de aquella operación del FBI. Trabajaba con un gran equipo, pero él era quien había convencido a los jefes, pese a su profundo escepticismo, de que le permitieran seguir adelante. No solo estaba en juego la reputación de los federales y la obtención del presupuesto, sino también su trabajo.

Y entonces recordó cuál era su fuerte: las ventas. O mejor aún: la ingeniería social.

Cuando los foros empezaron a transmitir la noticia de que Dark Market pertenecía a los federales, Mularski se tranquilizó y se recordó a sí mismo que la autocompasión nunca beneficia a nadie. Se puso en contacto con Grendel, acaso el más misterioso de los usuarios de Dark Market. En la vida real, Grendel trabajaba para una importante empresa de seguridad alemana, pero también ofrecía sus servicios contra reembolso a destacados ciberdelincuentes. Dark Market dependía de su red privada virtual (RPV), que ofrecía garantías casi absolutas de anonimato; pero, aparte de eso, Grendel también había creado cuatro *shells*, programas mediante los cuales el usuario se vuelve del todo invisible.

Grendel le envió los registros de conexión a la página, en ninguno de los cuales se mencionaba a Pembrooke Associates. Mularski comentó tanto en Carders Market como en Dark Market que la única persona que había encontrado el registro de Pembrooke Associates era… Iceman. Utilizando sus técnicas de venta, Mularski el vengador apartaba de sí las miradas suspicaces y las centraba en Iceman.

Las erratas del papel con membrete detectadas por Matrix001 eran la guinda del pastel. Iceman era de sobras conocido por su tendencia a acusar a la ligera a cualquiera que lo irritase, y, durante su época al frente de Carders

Market, casi todo el mundo lo había irritado en un momento u otro. Eso hacía que tuviera pocos amigos. Al mismo tiempo, la idea de que Iceman hubiera podido volver a las andadas como confidente de los federales arraigó sin dificultades, y Mularski la suscribió con entusiasmo.

Lejos de destruir Dark Market, Iceman había logrado lo contrario. La página resurgió con más fuerza que nunca y obtuvo reconocimiento casi unánime como principal web tarjetera en lengua inglesa del mundo. Gracias a su ingenio, Mularski había conseguido evitar un desastre seguro.

20

UN PLAN BRILLANTE

JiLsi no cabía en sí de contento. Carders Market y Iceman seguían en pie, pero medio groguis después del contraataque sufrido a raíz de sus acusaciones contra Dark Market. La mayoría de los tarjeteros creía ahora (erróneamente) que Carders Market era la web tapadera y que Dark Market estaba limpia. De resultas de ello, Dark Market empezó a crecer de nuevo hasta un total de dos mil miembros.

Por supuesto, circulaban rumores de que tal vez, con respecto a los administradores de Dark Market, no era oro todo lo que relucía, pero para entonces las manadas de tarjeteros ya eran tan frecuentes como los «lobos solitarios» en los primeros días del pirateo informático. Y la manada le había vuelto la espalda a Iceman para correr a los pies de Dark Market.

En diciembre de 2006, los directores de Dark Market estaban realizando una labor inestimable. JiLsi estaba orgulloso de sus logros, por fin se había convertido en un respetado miembro de la familia y su eficaz y desinteresado trabajo era apreciado en su justa medida. Había reunido a un gran equipo: Matrix, Master Splyntr y Cha0 eran administradores de primera clase y todos los miembros confiaban en sus servicios fiduciarios. Shtirlitz y Lord Cyric aportaban apoyo y credibilidad. Ambos, además, tenían buen ojo para detectar a *rippers* y tramposos, y sabían cómo tratar a los carroñeros que se criaban en los sumideros de la red. El volumen de negocio de los usuarios era cada vez mayor, y los ingresos empezaron a rozar el techo de los días dorados de Shadow Crew y Carder Planet.

Habían pasado más de dos años desde la caída de Shadow Crew y se percibía cierta complacencia. Los «lobos solitarios», que ahora eran minoría en los foros, nunca bajaron la guardia y ponían sumo cuidado en no dejar pistas que los incriminasen. Recka, el rey del fraude en Suecia, evitaba escrupulosamente trabajar con tarjetas de crédito o débito estadounidenses, ya que eso lo hubiera puesto en la lista de las fuerzas de seguridad de ese país; con los suecos y el resto de los europeos no había problema, pero por nada del mundo les habría puesto el dedo en el ojo a los norteamericanos.

Pero muchos otros tarjeteros, sobre todo los más jóvenes, seguían medidas de seguridad más laxas, olvidaban encriptar sus conversaciones por ICQ y dejaban a la vista sus direcciones IP al no usar RPV ni sistemas de tunelación adecuados. Entretanto, en Pittsburgh, Mularski estaba ocupado en reunir una base de datos con un programa de creación propia, capaz de establecer referencias cruzadas entre las actividades de cada tarjetero; para ello, leía sus mensajes, anotaba sus ICQ y direcciones IP y, cuando era posible, las vinculaba a cuentas de E-Gold.

Sin saberlo los usuarios de esa herramienta de divisas digitales, desde febrero de 2006 las agencias del gobierno disfrutaban de libre acceso a los archivos de E-Gold, el método de transferencia de capitales preferido por los tarjeteros. Todo empezó con la detención en Florida de su fundador, Douglas Jackson, ante la sospecha de que el servicio se utilizaba para blanquear dinero. Sin embargo, a pocos ciberdelincuentes (acaso a ninguno) se les pasó por la cabeza desconfiar de E-Gold. Los rusos, por su parte, preferían evitar las empresas occidentales, aunque estuvieran registradas en Belice, y confiar en Webmancy, con sede en Moscú y, por lo tanto, fuera del alcance de los agentes de la ley occidentales.

Una vez provisto de todas aquellas pruebas, entre el otoño y el invierno de 2006 Mularski se puso en contacto con los cuerpos de policía de varios países europeos. Mantuvo conversaciones con la Agencia contra el Crimen Organizado (SOCA) de Reino Unido, la policía federal alemana y, más tarde, con la policía regional de Baden-Württemberg.

Asimismo, entró en contacto con la OCLCTIC de París, la Oficina Central para la Lucha contra los Crímenes Relacionados con las Tecnologías de la Información y Comunicación, órgano de creación reciente y denominación algo pedestre. Ahí le dispensaron un trato más bien frío. La policía francesa suele colaborar de buen grado con Estados Unidos, sobre todo en asuntos de terrorismo y delincuencia informática, pero la tradicional suspicacia con respecto a los norteamericanos y sus intenciones en Europa está todavía muy arraigada en la sociedad francesa. Cualquier gobierno que dé la impresión de querer quedar bien con Estados Unidos corre el peligro de pagarlo en el terreno electoral, por lo que sus instituciones tienen orden de andarse con pies de plomo a la hora de tratar con Washington.

El director de la OCLCTIC, Christian Aghroum, consideraba ridículo que cada vez que él o sus agentes solicitaban ayuda a una empresa como Microsoft se arriesgaran a una protesta, como si ello fuera la prueba de que la policía estaba al servicio de las grandes corporaciones estadounidenses. La

realidad —y Aghroum lo sabía— era que nadie podía combatir la delincuencia informática a menos que mantuviera cierto grado de colaboración con empresas como Microsoft. Observador lúcido y perspicaz de los campos de minas que rodean la política internacional, Aghroum aceptaba con resignación el hecho de que ni los políticos ni la ciudadanía de Francia tenían la menor idea sobre la ciberdelincuencia ni sobre cómo combatirla. La mayoría de los franceses parecía convencida de que es posible luchar y reprimir la delincuencia transnacional sin salir de las propias fronteras, sobre todo cuando los delincuentes en cuestión no hablan francés.

Pero Mularski había de encontrarse con una sorpresa mucho mayor que el proverbial antiamericanismo galo: según le dijeron, la OCLCTIC llevaba varios meses colaborando con el Servicio Secreto en un caso relacionado con… Dark Market. Alguien estaba realizando una investigación paralela y nadie lo había informado al respecto. Por si fuera poco, el Servicio Secreto no daba muestras de querer compartir la información de que disponía. Pocos meses antes, el director de la División de Investigaciones Criminales del Servicio de Inteligencia había testificado ante el Congreso que, gracias a la estrecha colaboración con «otros cuerpos federales, estatales y locales, […] disponemos de una vasta red de información, recursos y conocimientos compartidos». Por lo visto, olvidó hacérselo saber al equipo que investigaba a Dark Market, ya que este incluso se negó a informar al FBI de cuál era el objeto de sus pesquisas. Las cosas se complicaban tanto para los ciberpolicías como para los ciberladrones.

Por entonces, la gran preocupación de los usuarios de Dark Market (a excepción de los que colaboraban con Mularski) no eran los agentes de la ley, sino cómo librarse de una vez por todas de Iceman para consolidar la supremacía de la web. JiLsi se arrogó la responsabilidad de asestar el golpe definitivo. Si lo lograba, se llevaría la gloria y su reputación aumentaría considerablemente. Por otro lado, estaba harto de las continuas incursiones de Iceman, que tanto trabajo extra le acarreaban, y la incendiaria retórica característica del *hacker* también empezaba a atragantársele.

El plan de JiLsi era muy simple. Creó una cuenta de correo anónima para mandar mensajes al proveedor de servicios de internet de Iceman. En ellos advertía al PSV que Carders Market, página a la que daba alojamiento, era una web delictiva y que sus propietarios se hallaban involucrados en estafas de gran calibre. Cuando Iceman descubrió la cuenta desde la que se enviaban los correos inculpatorios, se le ocurrió probar la contraseña de JiLsi («MSR206», el nombre de la legendaria máquina clonadora de tarjetas que

utilizaban todos los buenos tarjeteros), y —*¡voilà!*— funcionó. Iceman había descubierto que JiLsi estaba difamándolo ante su propio PSV. Aquello era imperdonable. JiLsi había traspasado una línea que ningún tarjetero (des)honesto debería cruzar nunca, por malas que sean sus relaciones con nadie: había denunciado a un miembro de la hermandad. Peor aún: había sido descubierto en plena delación.

Iceman hizo circular la noticia por todas partes. Al poco tiempo, llegó a oídos de Cha0.

Después de las acusaciones de Iceman, todo el mundo estaba aún un poco nervioso. ¿Estarían implicados los federales? Y lo que es más: si lo estaban, «¿quién cojones estaba trabajando con ellos?», por decirlo con palabras de uno de los administradores de Dark Market. ¿Iceman, Splyntr, c0rrupted0ne o silo, de Dark Market? ¿Shtirlitz, el enigmático «ruso»? ¿O quizá Lord Cyric, el nuevo moderador de Dark Market? ¿Tal vez otra persona?

Los únicos a los que hasta el momento nadie había acusado de trabajar para la policía eran Matrix001 y JiLsi. Este último había sido acusado alguna que otra vez de incompetente (y no sin razón), pero ¿de trabajar para la policía? Nunca. Iceman conocía la contraseña de JiLsi desde hacía tiempo gracias a sus incursiones pirata, pero ahora parecía ser de dominio público. Cundió la sospecha de que una tercera persona hubiera podido introducir un troyano en el inseparable lápiz de memoria de JiLsi y vigilar todos sus movimientos, lo que le habría permitido conocer los secretos más recónditos de Dark Market. O quizá JiLsi no era quien decía ser… ¿Mantendría algún tipo de vínculo con Pembrooke Associates, la misteriosa empresa del 2000 de Technology Drive?

Unos días antes de la Navidad de 2006, JiLsi se conectó a Dark Market como de costumbre para echar un vistazo al tráfico. Poco después, se desconectó para atender unos recados en el mundo real. Por la tarde volvió a conectarse. «Nombre de usuario: JiLsi —tecleó—. Contraseña: MSR206». Acto seguido, la máquina le devolvió el siguiente mensaje: «Nombre de usuario o contraseña incorrectos». Sin darle importancia, JiLsi volvió a intentarlo, achacándolo a un error de tecleo. El resultado fue el mismo. Lo intentó otra vez, y otra, y otra.

No cabía ninguna duda: JiLsi, líder espiritual y administrador jefe de Dark Market, había sido expulsado de su propia web. Estremecido de pánico, intentó conectarse a www.mazafaka.ru. Imposible. A The Vouched —otra de sus webs—; nada.

De pronto empezó a temblar. JiLsi jamás se había encontrado ante un abismo tan profundo. Acababan de robarle la vida entera, o por lo menos lo único que de verdad tenía sentido para él. Estaba furioso, dolido, disgustado. ¿Quién le había hecho eso y por qué? Reaccionó entregándose a las propiedades anestésicas del Martell y la pipa de crac. El dolor remitió durante la tarde y la noche, pero cuando se despertó se sentía más desgraciado aún que el día anterior.

Finalmente, JiLsi consiguió establecer contacto con Cha0 por ICQ. La conversación lo dejó fuera de juego: «Sabemos que has estado trabajando para Scotland Yard y la Unidad de Crímenes Tecnológicos —le espetó Cha0 —. Que decidieras delatar a Iceman no hace más que confirmarlo. Sabemos que trabajas con la policía. Has sido expulsado de todas la webs».

JiLsi se quedó sin habla. Todo aquello por lo que había trabajado había desaparecido en un abrir y cerrar de ojos, y, por si fuera poco, quien lo pagaba era él. ¿Qué sería lo siguiente? ¿Adónde ir? La situación era desesperada y JiLsi se sentía impotente.

PARTE V

21

DRON: EL LEGADO

Calgary, Alberta, 2006

Desde sus primeros días en Shadow Crew, el trabajo de Dron siempre le había reportado comentarios elogiosos. «Recibí la clonadora de Dron ayer por la mañana —comentaba en Dark Market un cliente satisfecho—. Pasé la tarde probándola y estoy más que impresionado. El material de Dron es de primera calidad, vale la pena invertir tiempo y dinero en él».

Dron no defraudaba a sus clientes: «El envío fue rápido, y el paquete era discreto», seguía el comentario. Pero si Dron se había hecho popular, no era gracias a sus envíos, sino por la atención posterior que dispensaba a sus clientes, que siempre acababan repitiendo: «Pero, en mi opinión, si en algo destaca Dron, es en el servicio al cliente. Envía actualizaciones a sus compradores con regularidad y siempre que le escribo con inquietudes o dudas recibo contestación en menos de veinticuatro horas. Impresionante de verdad».

En parte gracias a internet, la cultura de los derechos y expectativas del consumidor ha terminado haciéndose un hueco en el mundo de la delincuencia. Si un vendedor tima a un delincuente por internet, no es fácil encontrar al culpable para emplear con él el método por el que suele expresarse el descontento por un servicio deficiente, esto es, la violencia física. Pero los delincuentes que se dedican a la venta de productos ilegales por internet prefieren competir viendo quién ofrece mejor servicio.

En otra época, Dron habría medrado a toda velocidad. Había dejado la escuela a los quince años, pero combinaba su olfato para los negocios con cierta vena creativa. Su padre le enseñó a jugar a la bolsa por internet y, poco después, descubrió los foros de delincuencia informática. En la primavera de 2004, con veinticuatro años, ingresó en Shadow Crew, el más celebrado entre los predecesores de Dark Market.

Sin embargo, su mayor distintivo era una habilidad innata en temas de ingeniería. Aprendió solo y desde cero a diseñar y construir clonadoras

compatibles con los dos modelos más comunes de cajero automático. Eran dispositivos complejos e intrincados, pero valían hasta el último centavo de los cinco mil dólares que costaba cada uno (con descuentos por compras en grandes cantidades, por supuesto). Dron no solo atendía las consultas de sus clientes, sino que enviaba cada producto acompañado de un manual de instrucciones, el *software* requerido y un cable USB.

También su biblioteca daba fe de la seriedad con que enfocaba el negocio. Al lado de *Document Fraud and Other Crimes of Deception* podían encontrarse *Holograms and Holography* y *Secrets of a Back Alley ID Man*. Pero seguramente su volumen más preciado era *Methods of Disguise*. Cuando pasaba por una de las muchas cafeterías de internet de la ciudad para gestionar sus ventas y negocios en la red, Dron solía llevar gorra de béisbol y chaqueta negras. En cambio, cuando iba a la oficina de correos o cuando retiraba el dinero de una tarjeta de crédito en pago por una de sus clonadoras, prefería gorra roja y cazadora azul.

El Servicio Secreto estadounidense le había echado el ojo a Dron por su importante presencia en Shadow Crew. El administrador de Shadow Crew, CumbaJohnny, era un confidente del Servicio Secreto, pero Dron no pertenecía a la red privada virtual de CumbaJohnny, el medio principal por el que el Servicio Secreto controlaba la actividad de los miembros de la página. Como no residía en Estados Unidos ni era un objetivo fácil, no formaba parte de la lista de prioridades. Pero el Servicio Secreto no se olvidó de Dron. Al contrario, empezó a trabar relación con él.

Pese a su juventud en comparación con el Servicio de Inspección Postal estadounidense, el Servicio Secreto es el cuerpo que lleva más tiempo luchando contra la delincuencia telemática. Se formó en 1865, pero no para proporcionar protección armada al presidente, que fue uno de los principales reproches que le dirigió el Congreso tras el asesinato del presidente McKinley en 1901. Su fin originario, y lo es todavía hoy, era descubrir, investigar y perseguir a los productores o traficantes de dinero falso. Poco después de su fundación, el Congreso le encomendó asimismo las investigaciones de fraude financiero.

Tras la segunda guerra mundial, los acuerdos de Bretton Woods asentaron a Estados Unidos como líder indiscutible de las economías occidentales e instituyeron el dólar como moneda de reserva del mundo capitalista. Aunque la Unión Soviética y China rechazaron la preeminencia del dólar, las dos superpotencias comunistas se lanzaron a acumular el máximo de billetes verdes posible. En un mundo en el que la mayoría de los gobiernos

controlaban con mano de hierro el flujo de divisas a través de sus fronteras, la omnipresencia del dólar como forma de pago hizo que muchos se sintieran tentados de falsificar moneda estadounidense.

El resultado, en vista de que granujas y gobiernos del todo el mundo intentaban enriquecerse o socavar el poder norteamericano imprimiendo dólares por cuenta propia, fue la internacionalización de las operaciones del Servicio Secreto. Dondequiera que se encuentre, el lector de este libro puede estar seguro de que sus agentes se hallan en las proximidades. Sin embargo, y a pesar del largo brazo del Servicio Secreto, existen rincones a los que ni siquiera él puede llegar; buen ejemplo de ello es la difusión del «superdólar» en la década de 1990. Según el gobierno estadounidense, aquellos billetes de cien dólares falsos, aunque de extraordinaria semblanza, salieron de las prensas de Corea del Norte, una de las zonas que escapan a la vigilancia de los hombres de negro.

Por si salir al paso de las balas del presidente y perseguir billetes de pega no fueran trabajos lo bastante duros, en 1984 el Congreso solicitó ampliar las actividades del Servicio Secreto para incluir en ellas la investigación de fraudes con tarjetas de crédito y débito, la falsificación de documentos y el fraude informático.

A lo largo de las dos décadas siguientes, el que en cierto modo es el organismo de seguridad más secreto de Estados Unidos se especializó en la ciberdelincuencia, y adquirió una capacidad operativa sin parangón. Sin embargo, el Servicio Secreto solo tiene en nómina a seis mil quinientas personas. El FBI, por ejemplo, dispone de una plantilla de casi treinta mil. Recientemente, el Servicio Secreto ha sido absorbido por el Departamento de Seguridad Nacional, lo cual ha hecho estragos en su amor propio. Ambos cuerpos no se soportan, aunque es difícil saber si a causa del complejo de inferioridad del Servicio Secreto o de los delirios de grandeza del FBI; probablemente un poco de cada. Sea cual sea la razón, las riñas son constantes y repercuten en el resultado de las operaciones.

Tras la desarticulación de Shadow Crew, el Servicio Secreto decidió cultivar la relación con Dron, quien a finales de 2005 se había unido a Dark Market, donde su reputación como vendedor de clonadoras aumentó a tal velocidad que pronto creó su propio sitio web: www.atmskimmers.com. Durante varios meses, la oficina del Servicio Secreto en Búfalo se consagró a dar con su paradero. Dron utilizaba el servicio de correo israelí Safemail porque sabía que la compañía bloqueaba la dirección IP del remitente, lo cual significaba que el destinatario no podía acceder a él. El Servicio Secreto dio

por fin un paso adelante en enero de 2006, cuando Safemail accedió a revelar las direcciones IP de Dron después de que la solicitud del Servicio Secreto lograra abrirse paso en el inaccesible sistema penal israelí. Dron, según se supo entonces, operaba desde varios ordenadores repartidos por la zona de Calgary, en la petrolífera provincia de Alberta.

Los dieciocho meses siguientes fueron agotadores para el detective Spencer Frizzell, del cuerpo de policía de Calgary. Cada vez que Dron enviaba un correo al agente encubierto, Safemail enviaba una dirección IP a las oficinas del Servicio Secreto en Búfalo y Vancouver, que desde ahí era remitida a Frizzell. Las direcciones correspondían siempre a alguna cafetería de internet. Cuando se obtenía la localización exacta, el pájaro, naturalmente, ya había volado. Hasta hacerse con aquel caso, el detective Frizzell desconocía la existencia de tantas cafeterías de internet en Calgary y lo populares que eran. Cuanto más pasaba el tiempo, más le parecía estar buscando una aguja en un pajar.

Durante meses, dio la impresión de que Dron seguía patrones aleatorios. Un día aparecía en una cafetería; al día siguiente, en otra a cinco kilómetros. A veces desaparecía de Calgary y surgía el temor de que hubiera abandonado la ciudad, aunque siempre terminaba reapareciendo. Al cabo de unos meses, Frizzell hizo un gran descubrimiento. Gracias a las banderitas que iba colocando en un mapa, se percató de que todas las cafeterías de internet de Dron se hallaban cerca de las paradas de tren de cercanías, en la línea que va de Somerset a Crowfoot. Se fijó asimismo en dos o tres locales que Dron parecía preferir.

Con esa información ya podía enviar un equipo se seguimiento, pero encontró las típicas objeciones con que tropiezan todos los ciberpolicías en cualquier parte del mundo. ¿Quiénes son las víctimas en Calgary? ¿Qué pruebas hay de que esté lucrándose con una actividad delictiva?

Frizzell obtuvo la autorización, pero solo por un tiempo limitado y con muy pocos recursos humanos. Generalmente, cuando el Servicio Secreto le avisaba que Dron estaba en línea, se llevaba al primero que encontraba en la oficina y se dirigían a algún lugar de la línea del ferrocarril.

El detective de Calgary realizó una labor heroica durante más de un año, descartando sospechosos hasta convencerse de que había dado con su hombre. Lo que no sabía era que él no era sino un apéndice más de una operación a mayor escala del Servicio Secreto que no solo incluía a Dron, sino también a varios objetivos en Europa. El Servicio Secreto estadounidense había contactado con la SOCA de Londres y el OCLCTIC de París. «Nosotros

operamos así —afirma Edwin Donovan, portavoz del Servicio Secreto—. Nos esforzamos al máximo por colaborar con las policías de todo el mundo. Acudimos al cuerpo responsable de ese tipo de delitos y le informamos de que perseguimos a tal objetivo. Evidentemente, compartir la información es determinante en casos como estos».

Como se ve, el Servicio Secreto compartía información con las policías de Gran Bretaña, Canadá y Francia, pero no con sus colegas del FBI. Las evidentes rencillas entre los dos cuerpos llenaban de estupor a los europeos; a fin de cuentas, Francia colaboraba con el Servicio Secreto; Alemania, con el FBI, y Gran Bretaña mantenía un diplomático equilibrio entre ambos. Este estado de cosas desembocó en una situación sumamente irónica, en la que los únicos que sabían que el FBI y el Servicio Secreto tenían las miras puestas en la misma persona —JiLsi— eran los miembros de una fuerza policial extranjera, la Agencia contra el Crimen Organizado de Londres. La situación se deterioró más aún cuando la SOCA descubrió que, de hecho, los agentes encubiertos de un cuerpo eran considerados como presuntos delincuentes por parte del otro. Al final, un funcionario británico tuvo la sensatez de señalar a una instancia superior de Washington que quizá el FBI y el Servicio Secreto debían dejar de lado sus diferencias, por lo menos mientras durase la investigación.

22

MUCHACHO, ESTÁS JODIDO

Baden-Württenberg, 2007

Era una tarde apacible de principios de mayo, pero Matrix001 no estaba de un humor muy primaveral. El mundo exterior se hundía, tenía la boca seca y sus ojos recorrían el mensaje una vez más:

> Tu teléfono fijo está intervenido.
>
> La policía de Gran Bretaña, Alemania y Francia va a por ti. […] Esconde las pruebas. Avisa a los demás. […] Los polis saben que Matrix-001 es Detlef Hartmann de Eislingen […].
>
> Dentro de unas semanas la policía actuará en Gran Bretaña y Francia […].
>
> Avisa al máximo de tarjeteros posible.

¿Qué significaba eso? ¿De quién provenía el mensaje? Examinó otra vez la dirección del remitente: auto432221@hushmail.com. Seguramente una dirección creada de forma aleatoria. Imposible averiguar nada sobre el emisor, excepto que parecía poseer un buen dominio del inglés.

Matrix decidió que lo mejor era consultar con los demás administradores de Dark Market y un par de confidentes más. ¿Por qué le hacían eso?, les preguntaba. Sus respuestas, sin embargo, fueron extrañamente anodinas, en algunos casos casi indiferentes, meras invitaciones a mantener los ojos abiertos.

En Pittsburgh, Keith Mularski no se sentía ni mucho menos indiferente. Los extractos que Matrix les había enviado a él y a los demás solo podían significar una cosa: que alguien había filtrado la noticia de la operación. Y si Matrix había recibido una filtración, ¿quién más podía estar recibiéndolas? El momento no podía ser más inoportuno, ya que el FBI llevaba varios meses planificando la primera oleada de detenciones contra el entorno de Dark Market. Bastante tenía con lidiar con el Servicio Secreto. La policía alemana del estado federado de Baden-Württenberg (la LKA) había oído que sus

colegas franceses estaban preparando un operativo relacionado con Dark Market, pero los franceses les habían vuelto la espalda diciendo que su presencia en una reunión de planificación celebrada en París con la SOCA y el Servicio Secreto no era necesaria.

El mensaje anónimo recibido por Matrix001 tuvo a las fuerzas de policía con el corazón en un puño durante varios meses. Necesitaban saber si la filtración era resultado de una negligencia o de un topo, o si podía ser incluso que un *hacker* hubiera penetrado en alguna de las redes de los equipos de investigación. Cada vez que algo salía mal, afloraba la sospecha de que pudiera haber un traidor en sus filas, y la moral no podía por menos de resentirse.

Los intentos de Mularski por coordinar las primeras detenciones estaban hallando dificultades. Todo ciberpolicía teme que, al atrapar a un estafador, la noticia de que algo marcha mal se propague como la pólvora por los foros y los demás objetivos se esfumen. De aquí el obsesivo secretismo del Servicio Secreto…

«Espera un segundo —pensó Mularski—, seguramente la fuente de la filtración es… ¡el Servicio Secreto!». Examinó con atención a los posibles culpables: a) el Servicio Secreto; b) alguien de su propio equipo, cosa improbable dado que el FBI había incrementado la seguridad desde que Iceman descubriera la participación de los federales; c) la SOCA, que conocía a Matrix, aunque los británicos se caracterizan por su hermetismo, y d) por supuesto, los alemanes. Carecía de elementos de juicio acerca de los alemanes, pero le parecía haber detectado una relación un tanto tensa entre la fuerza regional de Stuttgart y la policía federal de Wiesbaden —a un par de horas de carretera en dirección norte—, dos cuerpos que conocían la existencia del caso Dark Market.

Por el momento lo mejor era dejar las especulaciones a un lado. La preocupación inmediata de Mularski era ponerse en contacto con Frank Eissmann, de la policía regional de Stuttgart, y ver cómo iba la investigación sobre Matrix antes de que el joven alemán pudiera poner tierra de por medio. En Stuttgart eran partidarios de dar un paso adelante y Eissmann propuso una fecha para la detención de Matrix. Eso, a su vez, creaba problemas a las policías de Londres, Calgary y París, que en la reunión en Londres a principios de abril habían acordado echar el guante a sus sospechosos el mismo día: el 12 de junio. La SOCA se sentía algo incómoda porque el Servicio Secreto llevaba vigilando a JiLsi desde los tiempos de Shadow Crew. Tanto los federales como el FBI no veían la hora de atraparlo.

Sin embargo, Matrix no escapó. De hecho, las conversaciones y los correos que la policía alemana interceptaba indicaban que el mensaje anónimo no lo había inmutado. ¿Habría sido prematura la decisión de acelerar la detención de Matrix?

Justo una semana después del primer correo, el 10 de mayo, recibió un segundo mensaje. Esta vez el emisor era auto496064@hushmail.com, que parecía un tanto molesto:

> Muchacho, estás jodido.
>
> Nuestra red os mandó un aviso a los tarjeteros alemanes, y ¿qué haces? ¡Hablar con el puto FBI!
>
> Eres tan imbécil que te mereces ir a la cárcel.
>
> El caso es que hemos interceptado varias comunicaciones entre el FBI y un alemán que se hace llamar Iceman. Te han puesto un cebo a través de un poli infiltrado que está a la espera de que compres o vendas algo. Todavía no sabemos su nombre. Pero quizá tú puedas ayudarnos a desmontar su tapadera.
>
> Y hazte un puto favor. Hasta que no sepamos quién es el poli infiltrado, no le compres nada a nadie.
>
> Como has sido tan listo de decirle al FBI que estamos en guardia, ¡es posible que ataquen antes! Borra toda la información de tu ordenador personal, aunque esté encriptada, y haz el puto favor de usar *solo* los de las cafeterías de internet.

Matrix se resistía a creer lo que decía la carta e hizo caso omiso de ella. Se convenció de que todo aquello era una farsa, como lo del caso Iceman. La policía, sin embargo, estaba cada vez más nerviosa. Como la conexión de Detlef Hartmann estaba intervenida, cuando este abrió el correo la policía también pudo leerlo. Frank Eissmann (a quien el misterioso auto496064 confundía con Iceman) no podía creer que hubiera alguien vigilando todas las comunicaciones de Dark Market. Los agentes empezaron a temer que toda la investigación sobre Dark Market pudiera haber sido pirateada y que los villanos estuvieran al corriente de lo que la policía sabía.

Mularski tampoco sabía qué pensar. Aunque había descubierto una anomalía importante: el anónimo autor del correo dominaba perfectamente el inglés, pero escribía *favour* con *u*, así que no podía ser estadounidense. ¿Quién podía ser?

23

FALLO DE MATRIX

29 de mayo de 2007. Empezaba el martes para los habitantes de Eislingen, una de las incontables poblaciones anónimas de Alemania donde la avería de un semáforo o la desaparición de una vaca pueden convertirse en la noticia del mes. Eislingen sigue una rutina que rara vez se interrumpe. En Alemania, la vida empieza una hora o dos antes que en Gran Bretaña o en Estados Unidos. A las seis y media de la mañana ya puede verse un reguero de personas de camino al trabajo o parando en alguna de las cafeterías de la cadena Tchibo. Ahí intercambian chismorreos mientras toman café cortado con un repugnante chorro de leche condensada, compensado gracias a las cremosas tartas o los *Weggle* de jamón ahumado (rollos de pan en el incomprensible dialecto suabo).

Y, sin embargo, aquel estaba destinado a ser un día especial en Eislingen. El siglo XXI estaba a punto de irrumpir. En la calle H., Detlef Hartmann se levantó de la cama sabiendo que debía hacer algo importante, aunque no lograba recordar qué. Mientras las brumas de su cabeza se disipaban, revisó su cuenta de Hushmail para ver si había mensajes encriptados y escaneó su página web por si necesitaba mantenimiento. No encontró nada fuera de lo normal.

De pronto se acordó. Sus padres volvían de pasar las vacaciones en Austria. Todo el mundo a sus puestos: él y su hermano tenían solo un día para limpiarlo todo. Los espaguetis resecos se agarraban a los platos como si fueran cemento industrial; montañas de colillas llenaban los ceniceros repartidos sin orden ni concierto entre latas de cerveza, botellas y prendas de ropa no identificadas; un buen cuadro, como el que pintan todos los adolescentes a la que se los deja sueltos. Detlef decidió darse un baño rápido antes de ponerse con la limpieza, y estaba secándose cuando llamaron a la puerta. Dio un grito para pedirle a su hermano que abriera.

La irritación de Detlef por verse importunado a las nueve y media de la mañana no hizo sino aumentar cuando su hermano gritó algo acerca de la

firma de un recibo. Detlef bajó la escalera a grandes zancadas dispuesto a discutir con la cartera por haberse equivocado de dirección. «Habla con ella», dijo con impaciencia su hermano, que temblaba ligeramente por la corriente de aire, mientras Detlef se abría paso hasta el vestíbulo.

«Ese coche está mal aparcado», pensó con su sagacidad habitual al ver una furgoneta negra estacionada en la calle. Delante de la furgoneta estaba la cartera. Llevaba una corbata atada con un nudo pequeño y ceñido y, en la cabeza, una rígida gorra con visera. Daba la impresión de ser una trabajadora concienzuda.

La cartera hizo casi una reverencia al entregarle a Detlef un sobre de tamaño A4 con una mano y un bolígrafo con la otra. Al ir a coger el bolígrafo, ella retrocedió de forma abrupta. «¿Qué demonios…?», pero antes de que Detlef pudiera terminar de pensar la frase, cuatro hombres se abalanzaron sobre él y lo echaron al suelo con las manos en la espalda. «¡Queda detenido!», gritó uno, mientras, como salido de la nada, otro grupo de agentes entraba en la casa. Detlef se quedó donde estaba, vestido solo con la parte inferior del pijama. Llovía y hacía frío, unos diez grados centígrados. Sintió que una bota le presionaba el cuello contra el suelo y unas esposas de plástico se hundían en su piel, mientras él no dejaba de repetir: «¿Se puede saber qué pasa?», con la sensación de estar metido en una película de serie B.

Diez minutos después estaba sentado delante del detective Frank Eissmann, de la LKA de Baden-Württemberg. El agente contemplaba con ojos sombríos los detritos de la cocina, el epicentro de aquel caos adolescente. «Dios bendito, esto está hecho una pocilga», observó el detective. Detlef, a modo de explicación, dijo que sus padres estaban de vacaciones. «Se nota», murmuró Eissmann para sus adentros.

A continuación, el agente y el detenido pasaron unos minutos en silencio. El único ruido perceptible era el castañeteo de los dientes de Detlef. La puerta se había quedado abierta y, después de su paso por la lluvia, su temperatura corporal había caído en picado. «¡Los ordenadores siguen encendidos!», gritó de pronto alguien desde el piso de arriba.

Detlef comprendió por fin lo que ocurría. Sobreponiéndose al frío y la confusión, pensó a toda prisa y le preguntó al agente si podía ponerse algo de ropa. La pregunta tenía sentido, pues estaba aterido de frío. Eissmann vaciló. Muy bien, convino y, advirtiéndole que constituía una irregularidad, permitió que el muchacho fuera a vestirse.

Mientras subía las escaleras, el cerebro de Detlef no dejaba de repetir: «¡Apaga el ordenador! ¡Apágalo! ¡Desconéctalo! ¡Desconéctalo!». Detlef

sabía que la policía no conocía su contraseña, de modo que, si conseguía deshabilitar el ordenador, no podrían encontrar pruebas. En principio, mientras no obtuvieran la contraseña, no podrían demostrar nada.

En la habitación, uno de los colegas de Eissmann miraba el ordenador con los brazos separados como un guardameta para proteger el equipo de posibles interferencias. Al ir a ponerse una camiseta, Detlef tropezó y tiró del cable de alimentación, sacándolo del enchufe. El zumbido cesó. «¡Mierda, mierda! —gritó el agente—. El ordenador se ha apagado». Eissmann subió corriendo a la habitación. «Muy bien. Ahora sí que la has hecho buena; será lo último que hagas en una buena temporada», dijo, arrastrando a Detlef de vuelta a la cocina. Eissmann le puso delante un folio escrito en jerga oficial. Lo único que recuerda Detlef es que, garabateado a mano, ponía: «Sospechoso de formar parte de un grupo criminal organizado».

Aunque estaba que echaba truenos por la boca, el detective Eissmann permitió que Detlef conversara brevemente con su hermano. Le dijo que no se preocupase, que todo se arreglaría. El hermano no decía nada, pero lo miraba como si estuviera chiflado. Por último, antes de salir de la casa, Eissmann le preguntó a Detlef si quería llevarse algo. «¿Podría decirme qué puedo necesitar? —preguntó Detlef, algo perplejo—. Nunca me había ocurrido una cosa así antes».

Mientras miraba por la ventanilla del coche patrulla de camino a la comisaría, Detlef se acordó de los dos correos anónimos recibidos un par de semanas antes. ¿En qué estaría pensando? ¿Por qué no había reaccionado? De todos modos, no estaba muy seguro de qué podría haber hecho. No era ningún matón con casas francas y redes mafiosas a su disposición, sino un estudiante joven y más bien cándido. Apenas si sabía qué era una «conspiración» y mucho menos qué implicaba formar parte de ella.

Detlef seguía cavilando cuando el coche patrulla se detuvo delante de un gran edificio blanco al fondo de la calle Asperger —nombre muy apropiado—, en el distrito de Stammheim de Stuttgart, la capital de Baden-Württemberg. De haber alzado la vista hacia una de las ventanas de la última planta, habría visto la celda donde Ulrike Meinhof, la carismática líder de Fracción del Ejército Rojo, un grupo terrorista de izquierdas de los años setenta, se ahorcó en 1976.

Más tarde el presidio de Stammheim se había reconvertido en prisión solo para hombres, aunque la agente que lo acompañaba era una mujer. En cuanto los reclusos la vieron, empezaron a gritarle obscenidades desde sus celdas.

A cada paso, el miedo de Detlef ante su nueva situación iba en aumento. ¿Cómo era posible que un respetable muchacho de clase media se encontrara en esa tesitura? Había terminado la escuela con notas sobresalientes y estaba preparándose para la universidad. Sus padres lo adoraban y agradecían la ayuda que les prestaba con sus tres hermanos menores. Y ahora aquel muchacho inofensivo de Eislingen se encontraba en Stammheim, el centro penitenciario de peor fama de toda Alemania. Tras desnudarlo y cachearlo, los celadores le entregaron unas prendas de recluso varias tallas más grandes, pero no zapatos. El nuevo pijama le iba tan holgado que parecía un traje de pesca de río. Llegó la hora de comer, pero seguía sin hacerse a la idea de que había entrado ahí para quedarse. Estaba conmocionado. Poco a poco, empezó a comprender que aquella era la etapa final del breve viaje que había comenzado cinco años antes. El día anterior había cumplido veintiún años.

24

LA CONEXIÓN FRANCESA

Marsella, junio de 2007

Dado que habían perdido toda clase de contacto, las dos agencias de seguridad estadounidenses llevaron a cabo los operativos contra Dark Market en paralelo. Con la supervisión del Servicio Secreto, el detective Spencer Frizzell arrestó a Dron en Calgary cuatro días antes de que en el sur de Alemania se produjera la detención de Matrix, respaldada por el FBI.

Frizzell llevaba semanas acortando la lista de «sospechosos habituales» mediante visitas a las incontables cafeterías de internet desde las que Dron había trabajado. Finalmente, identificó a aquel muchacho de veintiséis años de aspecto normal y corriente que, según el día, usaba uno u otro de sus tres uniformes «informales». El objetivo vivía en un apartamento decente del centro de Calgary, bien comunicado, como era evidente, por la línea de tren ligero.

Sin embargo, ni el agente Frizzell ni el Servicio Secreto estaban preparados para lo que se les venía encima. El sospechoso, Nicholas Joehle, tenía un centenar de clonadoras en proceso de fabricación. Si las hubiera vendido todas, se habría embolsado quinientos mil dólares y habría obtenido cientos de tarjetas en blanco y hologramas listos para ser falsificados. Naturalmente, la mera posesión de esas máquinas no constituye delito, pero Frizzell podía dar fe de que Joehle había ganado unos cien mil dólares con su venta durante el periodo investigado, algo menos de doce meses.

Claro que una cosa es detener a alguien porque se sospecha que lleva a cabo actividades ilegales en internet y otra muy distinta ordenar las pruebas para poder presentar cargos. La naturaleza virtual y transnacional de la ciberdelincuencia provoca a menudo que la fiscalía rechace el caso y dificulta su exposición ante un tribunal. Fuera de Estados Unidos, las condenas impuestas en esta esfera aún embrionaria de la ley suelen ser más breves que las de los delitos convencionales, lo cual significa que las fuerzas policiales se ven obligadas a invertir abundantes recursos para obtener resultados más bien

discretos. El problema con alguien como Dron es que su éxito lleva aparejado un deterioro de la economía local y global. Las pérdidas que puede provocar un pirata experimentado como Dron son enormes. No obstante, los ciberdelincuentes activos se cuentan por decenas de miles, y solo unos pocos llegarán a ser detenidos.

Joehle era una persona taciturna y sin formación, pero dotada de talento. Su instinto empresarial, unido a sus habilidades como ingeniero, probablemente lo ayude a levantarse una vez que reciba la sentencia y cumpla la condena. El *hacker* había transmitido sus conocimientos a otros miembros de Dark Market, entre ellos uno cuyo objetivo era establecer una red de producción de clonadoras por medio mundo. Pero eso ya no era cosa de Dron ni del detective Frizzell: la velocidad con que la información circula por el lado oscuro de la red es una razón más para que los cuerpos policiales nacionales amplíen los cauces de comunicación con sus colegas de otros países.

Eliminados Dron y Matrix, la policía tendría que proceder con celeridad y caer sobre los demás objetivos antes de que los miembros de Dark Market se percatasen de la repentina, y en buena medida inexplicable, desaparición de dos de los piratas más activos. Ahí el Servicio Secreto partía con ventaja, ya que Cha0, como administrador de Dark Market, había expulsado a Dron del foro.

Mientras Dron fue miembro del foro, Cha0 hizo valer su autoridad para apropiarse de los secretos del negocio del joven ingeniero. En cuanto él y su equipo (pues Cha0 disponía de varios cómplices) descubrieron el truco, dio de baja la cuenta de Dron, del mismo modo que había cancelado la de JiLsi en diciembre de 2006. Dron no podría volver a anunciarse en Dark Market, y puesto que casi todos los otros foros habían ido cayendo en el transcurso de la batalla campal entre Dark Market y Carders Market, la estrategia de ventas del joven canadiense quedaba seriamente perjudicada. Con Dron fuera de juego, Cha0 dedicó todos sus esfuerzos a monopolizar la venta de clonadoras.

Como Dron estaba vetado en Dark Market, sus tres socios franceses —Theeeel, de cerca de París, y Lord Kaisersose y Kalouche, de Marsella— no podían saber que Spencer Frizzell lo había puesto fuera de circulación. El Servicio Secreto, sin embargo, no tenía la menor idea de cuándo la policía alemana pensaba detener a Matrix, con la ayuda de los federales. Era probable que, si de pronto desaparecía de los foros, los demás miembros de Dark Market se inquietasen.

Recka, desde Suecia, supo enseguida que la policía había pasado a la acción. Intercambiaba correos con Matrix a diario y no se creyó el mensaje divulgado por Matrix a principios de junio de 2007: «Mi madre ha sufrido un grave accidente, de modo que me ausentaré una temporada». Cualquier ciberladrón con un mínimo de rodaje habría deducido al instante que la policía se había apoderado de su alias (como en efecto había ocurrido) y que el aviso era falso.

Lord Kaisersose, Theeeel y compañía eran franceses, y eso los hacía distintos. Francia contribuía de una forma peculiar al negocio de la delincuencia telemática. Los delincuentes franceses son tan obstinadamente francófonos como sus demás compatriotas. La Academia Francesa, policía de la lengua del país, asistió con incomodidad al exponencial crecimiento del inglés como lengua franca global a lo largo de la década de 1990, pero se complacía en señalar que, en el mundo digital, la mayor parte de los *hackers* y los *geeks* hacían frente común contra el inglés, la principal fuente de impurezas lingüísticas.

Eso quiere decir dos cosas: la primera, que en Francia la delincuencia informática tuvo en su origen carácter genuinamente nacional y no global como en el resto del mundo. El país se había adelantado a internet con la aparición en 1982 de un efectivo dispositivo de comunicación llamado Minitel, capaz de transmitir textos a un monitor a través de la línea telefónica convencional. Gracias a ello, Francia mantenía con las tecnologías de la información una relación mucho más madura que la mayor parte del mundo. El sistema Minitel, con el cual los abonados podían consultar números de teléfono, examinar sus cuentas bancarias, enviar flores o intercambiar mensajes subidos de tono a través de las *messageries roses*, era mucho menos accesible a los *hackers* que internet, lo cual explica en parte por qué en Francia la red no eclipsó a Minitel hasta fecha reciente. De aquí que Francia fuera en un principio menos vulnerable a los contagios virales. Por lo demás, eran relativamente pocos los *hackers* franceses que invertían su tiempo en foros como Carder Planet, Shadow Crew y Dark Market.

La segunda consecuencia ha sido la mayor lentitud en la difusión del correo basura en Francia. Los ingresos son mucho menos tentadores que los generados por el envío de *spam* en inglés, español y, en los últimos tiempos, chino. El problema son las reducidas dimensiones del mercado. Y hasta hace poco, los ochenta y tantos agentes de la OCLCTIC ni se molestaban en investigar las amenazas con origen en otros países (a diferencia del ejército y los servicios de inteligencia franceses, que cuentan con avanzados equipos

informáticos). La operación Lord Kaisersose (el grupo de Marsella) y la operación Disco Duro (Dron y Theeeel) contribuyeron en cierta medida a que los agentes de la OCLCTIC expusieran ante sus mandos políticos la conveniencia de que la policía se implicase de forma más efectiva en la salvaguarda de la ley en el plano internacional. Quizá lo más chocante fue que las detenciones de la OCLCTIC —para las que se movilizaron docenas de agentes armados en Marsella y en las afueras de París— no recibieron cobertura de ningún tipo por parte de la prensa francesa: ni un solo artículo.

Cuando arrestó a Theeeel, la policía quedó ligeramente sorprendida al ver que apenas contaba dieciocho años, lo que lo convertía en el más joven de los miembros de Dark Market detenidos. Se había introducido en el negocio de las tarjetas con la intención de pagarse los estudios universitarios. Si algunas jóvenes consideran que la única manera de terminar sus estudios pasa por vender su cuerpo de forma ocasional, cabe esperar que también los jóvenes *geeks* se sientan tentados de redondear sus ingresos. Como Theeel muy bien sabía, cuando el dinero empieza a llegar, cuesta estar sin él.

Al principio, los agentes franceses creían que Lord Kaisersose pertenecía a una de las numerosas bandas de pequeños delincuentes que pueblan Marsella, la Odesa francesa: otro puerto fascinante con un ambiente muy característico (además de una gastronomía fabulosa). Durante sus pesquisas, la policía había descubierto que Dustin, uno de los cómplices de Kaisersose, era propietario de un restaurante situado a una hora de la ciudad y que había cometido delitos menores de estafa.

Sin embargo, cuando los agentes de la OCLCTIC, junto con la policía local marsellesa, irrumpieron en el apartamento del sospechoso, Hakim B., en el centro de la ciudad, descubrieron que Lord Kaisersose jugaba en otra liga. Además de disponer de una amplia variedad de ordenadores, el piso estaba amueblado con gusto y elegancia. Hakim no era un matón callejero, sino un *hacker* experimentado con un hermano, Ali B., que trabajaba en DHL. Pocos negocios tan apetecibles a ojos de los delincuentes informáticos como la mensajería internacional. Con Ali como topo en DHL, Hakim tenía medios de sobra para introducir y sacar mercancías y dinero de Marsella sin llamar la atención. Factor crucial, puesto que Hakim se encargaba de revender la mayor parte de los *dumps* de Maksik, el rey de los tarjeteros ucranianos.

En un periodo de dos años, Maksik llegó a venderle a Hakim los detalles de veintiocho mil tarjetas de crédito, con un valor en metálico de unos diez millones de dólares. Con la ayuda de su equipo —Ali, Dustin y una o dos personas más—, Hakim enviaba las tarjetas a cajeros automáticos del sur de

Francia, con cuidado de no usar nunca tarjetas francesas, solo estadounidenses. Si el Servicio Secreto no se hubiera puesto en contacto con la OCLCTIC, hoy en día Lord Kaisersose seguiría en libertad y sería muchísimo más rico.

25

EL HOMBRE INVISIBLE

Renukanth creyó que podía empezar una nueva vida. La expulsión de Dark Market le había provocado una depresión que había durado tres semanas. Para él, lo único importante en el mundo era aquella página que él había contribuido a crear desde cero, y de pronto le había sido arrebatada. A medida que el invierno de 2006 dio paso a la primavera de 2007, la aflicción inicial fue remitiendo y poco a poco lo embargó una extraña sensación de libertad. Encontró fuerzas para dejar el crac y la bebida; las brumas mentales empezaron a desvanecerse y volvió al gimnasio para intentar perder parte del peso que había ganado durante su absorbente etapa como administrador de Dark Market. Como JiLsi era bajito, de la noche a la mañana había pasado de estar delgado como un palillo a ponerse gordo como una pelota.

Pasadas unas semanas, envió una solicitud de readmisión a los administradores de Dark Market. Le fue concedida, aunque rechazaron su pretensión de volver a ser administrador. A cambio, le dieron el título honorífico —aunque sin más valor— de «miembro respetado».

Ya no poseía poder de vida o muerte sobre los miembros de la web, pero seguía contribuyendo a su buen funcionamiento. Un miembro había ideado un sistema de robo de tarjetas en un aparcamiento de Texaco en Portsmouth, en la costa meridional inglesa. Alguien había instalado una minicámara en el techo, justo encima de la máquina de pago, de modo que, al mismo tiempo que se clonaban las tarjetas, se grababa a los propietarios tecleando el número secreto. JiLsi, para su desgracia, aceptó ejercer como gestor fiduciario por hacerle un favor al miembro, y lo que es peor, le pidió a otro, Sockaddr, que se encargase de retirar el dinero de las tarjetas en Estados Unidos. El problema era que Sockaddr era el principal agente encubierto del Servicio Secreto en Dark Market.

De todos modos, la actividad de JiLsi en el foro era cada vez más esporádica; sus días de tarjetero se acercaban a su fin. Aún no sabía qué haría si lo dejaba, pero estaba convencido de que había llegado el momento de

enmendarse. Tenía que poner fin al desastre en que se había convertido su vida.

Además, un sexto sentido le decía que algo extraño estaba ocurriendo. Su vista, su oído y su olfato se mantenían en alerta a la espera del más leve susurro, como un ciervo ante el peligro. Creía haber divisado a un par de animales al acecho. Estaba seguro de haber visto con el rabillo del ojo a un par de leones merodeando por el Java Bean. Incluso inspeccionaba el cielo en busca de buitres volando en círculos.

¿Sería la paranoia o acaso sus dos vidas paralelas como Renu y JiLSi corrían el riesgo de colisionar? Sea como fuere, lo mejor era prever los posibles desenlaces. No podía seguir negándose a reconocer lo que era obvio: un coche aparcado demasiado rato frente a la cafetería, desconocidos que por raza o indumentaria no encajaban en el local. Un par de semanas después, Renu empezó a variar la ruta que seguía para ir al Java Bean y volver. No cabía duda de que lo seguían. Eran los leones.

En cuanto a los buitres, formaban parte de un equipo menos organizado, aunque igualmente peligroso, que le hacía llegar avisos relacionados con ciertas obligaciones financieras contraídas a raíz del desastroso episodio del lápiz de memoria del año anterior. Querían su dinero o su carne. ¿Estaría dispuesto a negociar alguno de los dos grupos? ¿O tendría que huir de ambos?

Mick Jameson había asumido el mando del caso de JiLsi un par de meses antes, en marzo. La Agencia contra el Crimen Organizado (SOCA), para la que trabajaba, llevaba más de medio año siguiéndole el rastro al *hacker* gracias a un soplo de Keith Mularski. Tanto el Servicio Secreto como el FBI hacía tiempo que iban tras los pasos de JiLsi debido a la compulsiva actividad de este en foros ilegales de todo tipo (hasta el punto de que, si el *hacker* no formaba parte en una web, la página perdía pedigrí). Su simpático avatar, el del pirata con parche y sombrero de tres picos, era incontenible.

La SOCA era el único cuerpo policial que tenía conocimiento de las operaciones tanto del FBI como del Servicio Secreto, y, hasta cierto punto, la unidad contra el crimen organizado actuaba como pacificador pasivo, garantizando al menos que la fecha de detención de Lord Kaisersose y Theeeel en Francia coincidiera con la de Matrix en Alemania y JiLsi en Inglaterra.

Desde febrero el Java Bean era vigilado por los micrófonos y las cámaras de uno de los equipos de investigación. Los agentes que seguían a Renu lo habían descubierto reuniéndose con unas cuantas personas, con las que a menudo hablaba en tamil; lo habían visto entregando dinero en metálico y

lápices de memoria a sujetos que llegaban en coche y partían sin apenas detenerse; incluso tropezaron con otro usuario de Dark Market que también frecuentaba el Java Bean. Pero a quien querían era a Renu. Habían sacado instantáneas de su pantalla con un teleobjetivo, y uno de los colegas de Jameson se había infiltrado en Dark Market haciéndose pasar por miembro ordinario, lo cual les permitía mantenerse al corriente de los mensajes de JiLsi. Además, Mularski les facilitaba una información preciosa. Pero, aun así, seguían sin dar con la prueba definitiva que identificase a Renukanth Subramaniam como JiLsi. Para eso sería necesario arrestarlo.

Los distintos cuerpos de policía decidieron ir a por él la segunda semana de junio. Por fin el Servicio Secreto y el FBI se ponían de acuerdo en algo: el 12 de junio sería el día D. Pero entonces el plan se frustró por culpa de los correos anónimos dirigidos a Matrix001. Si la detención de JiLsi fracasaba, era muy posible que en cuestión de minutos la noticia se difundiera por Dark Market, echando a perder varios años de minuciosos preparativos.

De pronto, los peores temores de Jameson se hicieron realidad: dos días después del arresto de Matrix, JiLsi se esfumó. Una mañana salió de casa, pero no para ir al Java Bean, sino a la cercana estación de Wembley Park, desde donde se dirigió al centro de Londres. A la altura de IKEA, en la Circular Norte —la carretera de circunvalación de Londres, siempre colapsada—, se fijó en un hombre de aspecto peculiar. ¿O era una mujer? No estaba seguro. Quizá lo mejor era definirlo como andrógino. Siguió caminando hacia Wembley Park. Al aproximarse al pasaje subterráneo, junto a la parada del metro, vio en el puente a un hombre de pelo largo que hablaba por teléfono sin quitarle los ojos de encima.

Tras tomar la línea de Jubilee en sentido ciudad, JiLsi cambió a la línea de Picadilly en Green Park para bajar por último en Leicester Square. Como a menudo ocurre en esa parada, salió por la boca equivocada y tuvo que deshacer camino hasta llegar a la plaza propiamente dicha.

De repente, el corazón le dio un vuelco: ahí mismo estaba don Andrógino. Y mientras cruzaba la plaza Leicester, atestada de turistas y artistas callejeros, Renu estuvo a punto de darse de bruces con don Pelo Largo. Ya no cabía ninguna duda: lo estaban sometiendo a una estrecha vigilancia.

Entró en un restaurante chino y, mientras devoraba la comida, consideró sus opciones. Salió de nuevo y embocó la calle St. Martin, un pasaje que se convierte en zona peatonal a la altura de la National Gallery y conduce a la plaza de Trafalgar.

Los turistas se arremolinaban en torno a la columna de Nelson para admirar la extraordinaria estatua de tres metros y medio de altura que ocupaba el cuarto pedestal, cuyas esculturas se cambian cada dieciocho meses aproximadamente. *Alison Lapper embarazada* representa, encinta y desnuda, a la artista británica del mismo nombre. Lapper nació sin brazos. En su momento, la decisión de exponer la estatua causó un revuelo considerable. La obra atraía a la multitud; Renu se abrió paso a través de la marea de turistas, con sus perseguidores pisándole los talones. Tomó el primer autobús que encontró y desde el piso superior vio a don Andrógino y a don Pelo Largo mirando con desesperación a su alrededor en busca de la presa desaparecida.

Renu se evaporó. Y no fue el único: JiLsi no volvería a colgar mensajes en la red.

Un par de semanas después, Renukanth se dirigió hacia una de las varias propiedades que, aunque no le pertenecían, tenía hipotecadas. Ya casi había llegado a la casa, justo debajo de la ruta de aterrizaje del aeropuerto de Heathrow, cuando le sonó el teléfono. Era un colega suyo que vivía ahí y le advertía que no se acercase. La policía acababa de entrar en la casa con una orden de arresto.

El oficial de la SOCA al mando de la investigación de JiLsi, Mick Jameson, ya había visitado el domicilio principal de Renu en Coniston Gardens y unos cuantos más. Aparte de su trabajo como JiLsi en Dark Market, el de Sri Lanka era un estafador hipotecario en serie. Había mentido de forma constante acerca de su situación profesional y financiera para conseguir que varios acreedores le prestasen dinero tomando como garantía varias fincas del norte, el oeste y el sur de Londres. Gran Bretaña no vivía la fiebre *subprime* que se había apoderado de la industria financiera estadounidense, pero el llamado sistema de autocertificación (según el cual la palabra de uno es prueba suficiente de sus ingresos), unido a la práctica de conceder préstamos por cinco veces el sueldo del solicitante (en tiempos de mayor cordura, la cifra nunca excedía el triple), facilitaba relativamente la comisión de ese tipo de fraudes. La competencia en el mercado era tal que mirar hacia el otro lado se había convertido en la estrategia favorita de la banca.

Pero en el momento de recibir la llamada, Renu estaba más preocupado por salir del cenagal en que se hallaba inmerso que por la letra pequeña de sus múltiples estafas. Sin pensarlo dos veces, decidió no volver a dar señales de vida. Pasó tres semanas durmiendo a la intemperie, evitando acercarse a las direcciones que suponía sujetas a vigilancia de algún tipo. Cuando lo

informaron de la incursión de la policía, llevaba encima unas quinientas libras.

Había llevado una vida frenética y arriesgada, pero a Renu siempre le había gustado vivir como un fantasma: cambiar de domicilio cada cierto tiempo, entregar lápices de memoria bajo mano a tipos de aspecto misterioso y, por supuesto, ser celebrado como un capitoste de las webs de tarjeteros, sin que nadie supiera quién era. Al principio, creyó que cubrirse con unos cartones debajo de un puente con un grupo de alcohólicos contribuiría a esa mística. Pero, a medida que se le acababa el dinero y su situación se iba deteriorando hasta la más pura miseria, Renukanth Subramaniam —débil, sucio y enfermo— vio que se aproximaba a un callejón sin salida.

El 3 de julio de 2007 se personó en la comisaría de Wembley Park y se entregó. La parte fácil de la operación Dark Market había concluido.

INTERLUDIO

EN EL PAÍS DE NO SÉ QUÉ NI DÓNDE

Tallin, Estonia

Cuatro días antes de las elecciones generales, en la primavera de 2007, el pequeño Estado báltico de Estonia, con una población de solo un millón doscientos cincuenta mil habitantes, ofreció a sus ciudadanos una primicia mundial: la posibilidad de depositar sus papeletas para las elecciones parlamentarias sin levantarse de delante del ordenador. Si el experimento salía bien, el objetivo era promover unas «elecciones virtuales» para cuatro años después, en 2011.

Si Estonia conseguía dar ese importante paso hacia el futuro digital, se plantearían muchos retos: no solo habría que garantizar el correcto funcionamiento de los sistemas, sino también su seguridad frente a un ataque externo. Un año antes, Estonia había presentado de forma oficial el Equipo de Respuesta ante Emergencias Informáticas (CERT), cuyo cometido principal era solucionar posibles vulneraciones (accidentales o deliberadas) en los dominios de internet con el sufijo del país: .ee. Para ello había que supervisar de forma constante el tráfico de internet que entraba, salía o circulaba por el interior del país, en busca de patrones anómalos.

El responsable de la seguridad informática estonia es Hillar Aarelaid, un tipo con voz queda y aspecto de acabarse de levantar de la cama sin muchas ganas. Pese a su aire distraído, Aarelaid es un hombre con una gran determinación gracias a la cual destacó en las filas de la policía estonia, donde empezó como agente de tráfico en una población remota. «Como me gustaban los ordenadores, primero me trasladaron a Tallin y, finalmente, me nombraron jefe de información de la policía del país». No debe sorprender, pues, que tenga aspecto de *geek*. Desde luego, no parece policía (a lo sumo un agente de narcóticos de paisano de los años ochenta), lo que hace pensar que su nombramiento al frente del CERT en 2006 podría obedecer, entre otros, a motivos estéticos.

El día de las elecciones virtuales de 2007, el CERT y los excompañeros de Hillar de la policía se hallaban en estado de alerta máxima. «Por fortuna —explica—, pues detectamos que alguien había lanzado un *botscan* contra el sistema de votación». Por lo visto, alguien había enviado una sonda automática con instrucciones de detectar si por error alguno de los puertos de

los servidores electorales había quedado abierto. «No fue nada grave, ya que los *botscans* son bastante fáciles de detectar —continúa Hillar—, pero aun así representaba una verdadera amenaza a la seguridad».

Dicho esto, saca pecho —todo el pecho que puede sacar alguien con la templanza de Hillar— y anuncia triunfante que «a los quince minutos de detectar el *botscan*, teníamos a un agente llamando a la puerta de un domicilio de Rapla, cincuenta kilómetros al sur de Tallin, y preguntándole al inquilino: "¿Puede saberse por qué ha lanzado un *botscan* contra los ordenadores electorales?"».

En el mundo de la ciberseguridad, que entre la detección de una fechoría y la llegada de un agente al lugar donde se halla el equipo malhechor medien quince minutos constituye una marca más que notable: una labor magistral. «Tuvimos la suerte de poder hacer un buen trabajo —admite Hillar—; cuando llegó el primer gran ataque, a finales de abril, ya estábamos bien preparados».

El «gran ataque», ocurrido dos meses después de las elecciones, fue otra «primicia» en Estonia. Las redes del país fueron víctimas de una ofensiva sostenida que obligó a cerrar los vínculos de internet con el mundo exterior. Para algunos, aquel fue el primer episodio de guerra informática de la historia.

Me puse a buscar a Hillar un mes después de mi visita a Google, en Silicon Valley. Mi viaje al Este me condujo hasta Tallin, la pintoresca capital del más septentrional de los Estados bálticos. La muralla de la ciudad vieja protege una rica mezcla de estilos arquitectónicos escandinavos, germánicos y eslavos, donde se ve que las antiguas aspiraciones imperiales de los vecinos del norte, el este y el oeste del país no dieron paso a una cultura verdaderamente nacional hasta hace apenas veinte años, tras la caída del comunismo (a pesar de que todavía una cuarta parte de la población tiene raíces rusas).

Pared con pared con las iglesias ortodoxas, luteranas y católicas, pueden encontrarse restaurantes turísticos decorados con un bucolismo impostado y, para después de la comilona, animados locales nocturnos para terminar la noche con un poco de baile. En Estonia se ven menos grupos de jóvenes ingleses borrachos que en la vecina Letonia, aunque no deja de tener una parte sórdida. Entre las discotecas, se encuentra el evocador Depeche Mode Baar, que solo pone música de la banda de Essex y constituye una especie de homenaje al legado cultural británico de los primeros días de Margaret Thatcher.

El ambiente extraño, aunque acogedor, de Tallin quedaba realzado por el hecho de que mi llegada se producía solo una semana antes del solsticio de verano y las legendarias noches blancas. La oscuridad no llega hasta justo pasada la medianoche y la luz reaparece una hora y media más tarde. Al cabo de una semana, la luz dura las veinticuatro horas del día.

Aquella encrucijada confusa de ambiciones imperiales, peculiares iconos culturales modernos y luz ensoñadora es el telón de fondo ideal para la reunión anual del Centro de Excelencia para la Ciberdefensa Cooperativa (CCDCOE), el centro que, bajo los auspicios de la OTAN, investiga la guerra informática en todas sus facetas. Los asistentes al congreso habitan un País de las Maravillas contemporáneo en el que a menudo las formalidades quedan a un lado: tipos con gafas metálicas y cola de caballo intercambian tranquilamente información acerca de «vulnerabilidades de inyección SQL» con militares de uniforme almidonado. Funcionarios trajeados conversan con jóvenes vestidos con vaqueros y camiseta sobre los perjuicios de los «ataques MitM».

Para captar por lo menos los rudimentos de la seguridad informática en toda su variedad, hay que estar dispuesto a aprender un sinfín de expresiones nuevas sujetas a continuas adiciones y variaciones. De lo contrario, el lego asiste a conversaciones cuyo vocabulario básico y estructura sintáctica reconoce de forma inequívoca como pertenecientes al inglés, pero que carecen de sentido para el profano. Evidentemente, resulta embarazoso preguntar una y otra vez a quienes manejan con soltura ese lenguaje misterioso por qué los «desbordamientos de *buffer*» pueden tener consecuencias nefastas para la seguridad de una red, pero la tribu de los *geeks* no suele ser engreída y por lo común responde gustosa.

Es posible que Estonia sea pequeña, pero es el país mejor conectado de Europa y una de las potencias digitales líderes en el mundo; de allí —entre otros inventos— procede Skype. En casi todas partes se puede acceder a la red sin cables y de forma gratuita, ya que la conexión se considera un derecho básico, no un privilegio. Allí los hoteles no lo despluman a uno por navegar por internet.

De todos modos, yo no había ido para hablar con Hillar Aarelaid sobre el papel pionero de Estonia, sino sobre su privilegiado lugar en la historia de la guerra digital internacional.

A principios de 2007, el gobierno estonio anunció su intención de trasladar el Monumento a los Caídos del Ejército Rojo durante «la gran guerra patriótica» (como los rusos llaman a la segunda guerra mundial) desde su

emplazamiento en el centro de Tallin hasta el cementerio principal de la ciudad, no muy lejos del centro. Los líderes rusos lo interpretaron como un insulto intolerable, e incluso vieron en ello una prueba del resurgimiento del nacionalismo fascista estonio (entre los setecientos cincuenta mil habitantes del país que no proceden de la inmigración) y un ultraje a los soldados del Ejército Rojo que sacrificaron sus vidas para liberar a Estonia del yugo nazi.

La disputa sobre el soldado de bronce fue subiendo de tono. Los medios rusos, tanto los de Estonia como los del otro lado de la frontera, alimentaban los miedos de la minoría rusa del país y, al poco tiempo, el asunto adquirió dimensiones críticas. La tarde del 27 de abril, cientos de jóvenes estonios de etnia rusa se concentraron en el centro de Tallin. La protesta contra el cambio de ubicación del monumento tuvo un carácter pacífico y festivo hasta que un grupo intentó romper el cordón policial que protegía la estatua. Los enfrentamientos no tardaron en extenderse, y, por la noche, en la ciudad vieja, calificada por la Unesco como patrimonio de la humanidad, hubo quemas de vehículos, roturas de escaparates y saqueos de comercios.

Los disturbios amenazaban con propagarse, y Moscú emitió comunicados en los que acusaba a la policía estonia de cometer abusos. El mismo país que dos décadas antes había conquistado la independencia de la Unión Soviética se veía ahora atenazado por la incertidumbre y el miedo. Era del todo improbable que Rusia ofreciera a Estonia «ayuda fraternal», por usar el eufemismo soviético equivalente a sacar los tanques a la calle. Después de todo, Estonia era miembro de la OTAN y parecía inconcebible que Rusia estuviera dispuesta a poner a prueba el lema de la organización —todos para uno y uno para todos— por una maldita estatua.

Por suerte para todos, el Kremlin no parecía inclinado a enviar ayuda fraternal, pero mientras en el centro de Tallin se sucedían incendios, tumultos y quemas de banderas, los *hackers* aprovecharon el conflicto para abrir un nuevo frente.

Esa noche, las webs del presidente de Estonia y de varios ministerios del gobierno empezaron a recibir cantidades exorbitantes de correo basura y la fotografía del primer ministro en la web de su partido fue manipulada. Por las salas de chat rusas circulaban llamamientos a que los *hackers* lanzaran ataques contra las webs estonias y se facilitaba el acceso a los programas necesarios para ello. Según fuentes citadas en un telegrama de la embajada estadounidense a Washington (filtrado a Wikileaks), los primeros ataques no presentaban ninguna sofisticación desde el punto de vista técnico y «parecían más una reyerta cibernética que una guerra informática».

El fin de semana, la lluvia de correos basura se convirtió en ataques DDoS. Los *hackers* crearon docenas de molestos *botnets* y reclutaron ordenadores zombis de todo el mundo para obligarlos a conectarse a las webs estonias, provocando ataques a gran escala; así, la página presidencial, «que de ordinario tiene una capacidad de dos millones de megabits por segundo, quedó inundada por un tráfico de casi doscientos millones de megabits por segundo», según el cable de la embajada estadounidense. La situación habría podido reconducirse, pero el 3 de mayo «los ciberataques se propagaron de las webs y los servidores del gobierno de Estonia a páginas y servidores privados».

Hacia las diez de la noche, Jaan Priisalu recibió una llamada en su domicilio, en las afueras de Tallin. «Me dijeron que iban a caer todos los canales», recuerda. Como jefe de seguridad y tecnologías de la información del mayor banco de Estonia, Hansabank, Priisalu se sentía impotente. «Al rato recibí un SMS en el que se me informaba de que nuestro servicio de banca en línea estaba colapsado».

Los ataques llegaban de todos los frentes: decenas de miles de equipos inundaban los sistemas de Hansabank con solicitudes de información. Priisalu escarbó sin perder tiempo en toda aquella frenética actividad electrónica y no tardó en descubrir que Hansabank se hallaba bajo el ataque de un *botnet* formado por unos ochenta mil ordenadores. Siguiendo los ataques hasta su origen, Priisalu averiguó que procedían de un servidor de Malasia. El resultado no era en absoluto concluyente, solo significaba que a partir de Malasia los atacantes habían conseguido enmascarar su origen real. Lo que sí estaba claro era que se enfrentaban a un ataque de gran virulencia. «Fue demoledor», afirma. Un *botnet* de ochenta mil ordenadores es un monstruo terrorífico capaz de paralizar por entero el sistema de una compañía en cuestión de minutos.

Gracias a las medidas cautelares de Priisalu, Hansabank disponía de potentes servidores y webs espejo con réplicas del contenido (lo que dificultaba el éxito de los ataques DDoS). No obstante, y a pesar de que Hansabank se mantuvo en línea, la principal fuente estonia de la embajada estadounidense informó que el incidente había tenido para la compañía un coste «como mínimo de diez millones de euros».

Los objetivos siguientes fueron los medios estonios, incluido el periódico más visitado de la red. «Imagínese —señala un observador—, si puede, el efecto psicológico sobre los estonios al ir a pagar una factura y no poder, o al intentar leer las noticias en la red y no conseguirlo». El gobierno estaba en

máxima alerta y muy preocupado ante la posibilidad de que los ataques plantearan «una alarmante amenaza a la infraestructura económica y social básica».

Gracias a la coordinación entre el gobierno, la policía, los bancos y el CERT, el impacto de los ataques sobre la ciudadanía se mantuvo dentro de límites razonables. Hansabank pudo mantener sus servicios en línea; los otros dos bancos principales no, pero para los clientes las molestias no pasaron de tener que personarse en las sucursales. Las redes de telefonía móvil quedaron interrumpidas y, tras la orden del gobierno de cortar todos los vínculos de Estonia con el extranjero, las comunicaciones con el país siguieron siendo difíciles durante unos días. Contrariamente a lo afirmado en los primeros informes, los semáforos de Tallin no dejaron de funcionar, aunque sí se registraron interrupciones en el trabajo del gobierno y de los medios.

La ofensiva se prolongó, con distinta intensidad, durante dos semanas, y culminó con un ataque masivo el 9 de mayo, fecha de la victoria del Ejército Rojo sobre los nazis en Europa. Agotado por el incesante torrente de ataques DDoS, el gobierno estonio decidió aislar el sistema de internet del país del resto del mundo. Poco a poco, las aguas volvieron a su cauce y los ataques cesaron por fin el 19 de mayo.

Los sucesos de Estonia tuvieron graves consecuencias. En lo político, era evidente que los ataques provenían de Rusia, pero como era de esperar Moscú negó toda relación con los hechos. Por otra parte, era posible que el Kremlin no estuviera involucrado de forma oficial. Los investigadores no consiguieron localizar con precisión el origen de la ofensiva. Si realmente provenía de Rusia, el gobierno, con su omnisciente sistema de control, el SORM-2, por fuerza tenía que saberlo, aunque la actividad cibernética alcanzaba en Rusia un volumen tal que cabe la posibilidad de que incluso el famoso SORM-2 tuviera dificultades para estar al corriente de todo. Quién sabe. Una de las cosas que el ataque a Estonia puso en evidencia es que puede conjeturarse quién anda detrás de sucesos como ese, pero difícilmente puede demostrarse.

Como los demás gobiernos, el ruso todavía estaba definiendo su actitud hacia internet, su función y la relación entre el Estado y el usuario final. Moscú se había percatado ya en la década de 1990 de que la importancia de internet en términos políticos y de seguridad era tal que merecía toda la atención de una de las instituciones más duraderas y exitosas del país: la policía secreta. Por eso el FSB (directo sucesor del KGB) desarrolló un medio para controlar todos los datos que entraban, salían o circulaban por el país. El sistema fue bautizado con el siniestro y significativo nombre de SORM-2,

siglas de Система Оперативно-Розыскных Мероприятий, o, lo que es lo mismo, Sistema para Actividades Operativas y de Investigación.

El funcionamiento del SORM-2 es francamente aterrador. Cuando alguien solicita información en la red desde su ordenador en Vladivostok o Krasnodar, dicha información es remitida al proveedor de servicios de internet correspondiente. Pero, además, la central del FSB en Moscú recibe un duplicado para que sus funcionarios puedan verla, sopesarla, reírse de ella o (quién sabe) utilizarla como prueba contra el usuario, según se le antoje. En el mejor de los casos, queda almacenada.

El SORM-2 no solo exige que los proveedores de servicios de internet remitan copia de *toda* su actividad al cuartel general del FSB, sino que añade el insulto a la ofensa obligando a dichos proveedores a comprar el equipo necesario (con un precio superior a los diez mil dólares) y a abonar los costes del servicio. Los costes, naturalmente, terminan sufragándolos los clientes, que de ese modo pagan de su propio bolsillo una potente herramienta de opresión de la que son la principal víctima.

El Estado ruso tiene autoridad para saber quién hace qué, cuándo, a quién y, quizá también, por qué en la red. Cabe, desde luego, la posibilidad de que un usuario avispado intente sortear al omnipresente SORM-2 encriptando sus datos y búsquedas de internet; pero no hay que olvidar que en Rusia el encriptado es ilegal y que un simple archivo con cerrojo digital puede acarrear un viaje solo de ida a Siberia.

Lo dicho no implica que los regímenes de internet de los gobiernos occidentales sean modélicos en cuanto a libertad de expresión. Al contrario, a medida que nuestra dependencia de la red aumenta, crecen también el deseo, la capacidad y la voluntad de los gobiernos de establecer un control férreo. Aunque funcionarios y políticos niegan a menudo la existencia de medidas a tal efecto, la lenta y dolorosa muerte de la privacidad electrónica en Occidente, sobre todo en Reino Unido y Estados Unidos, es una triste —amén de visible— realidad, y, acaso, algo inevitable.

La respuesta al 11-S mermó severamente nuestra libertad con respecto a las interferencias del Estado en la red en nombre de la lucha contra el terrorismo. En Estados Unidos, la herramienta principal para ello fue el Programa de Conocimiento Total de la Información (TIA). Pese a su proverbial ceguera, incluso la administración Bush se dio cuenta de que las connotaciones orwellianas del nombre eran demasiado evidentes y lo cambió por el de Programa para el Conocimiento de la Información Terrorista.

El TIA proporcionó al DARPA, el ala de investigación y detección del Pentágono, acceso a datos obtenidos de comunicaciones privadas. El programa terminó cerrándose, pero muchas de sus funciones fueron asumidas por el gobierno para luego redistribuirlas entre distintos organismos del país.

Por si fuera poco, el Tribunal Supremo, en un gesto histórico, dio luz verde al FBI para instalar registradores de teclas troyanos en los ordenadores de sus sospechosos; eso sí, siempre bajo la supervisión de un juez. De ese modo, el FBI puede controlar todas las operaciones realizadas con el equipo del sospechoso, lo mismo que hacen los delincuentes informáticos cuando infectan ordenadores de terceros. Además, a principios del nuevo milenio, el Parlamento europeo confirmó la existencia de Echelon, un programa estadounidense de espionaje global supuestamente capaz de almacenar comunicaciones digitales de cualquier lugar del mundo.

En el ámbito de la Unión Europea, durante la presidencia británica se publicó una directiva que obligaba a los proveedores de servicios de internet europeos a almacenar todo el tráfico informático (incluido el de los teléfonos móviles) durante un lapso comprendido entre seis meses y dos años. Los datos quedaban a disposición de los organismos gubernamentales, que podrían acceder a ellos aplicando la legislación vigente en cada país. Si esta tendencia a la vigilancia digital sigue su curso, los gobiernos occidentales (casi siempre en nombre de la estrategia contra el terrorismo y la salvaguarda de la ley) dispondrán cada vez de más recursos para controlar los movimientos y costumbres de sus ciudadanos.

Los investigadores de la London School of Economics han descrito como nadie el camino por el que vamos. En junio de 2009 invitaban al lector a imaginar que…

> … el gobierno tiene a un agente de seguridad sordo para cada persona, a la cual sigue adondequiera que va. Dicho agente no puede oír el contenido de las interacciones, pero observa hasta el último detalle de la vida de la persona: la hora a la que se levanta, el camino que sigue para ir al trabajo, la gente con la que habla y durante cuánto tiempo habla, el estado de su negocio, su salud, la gente que encuentra por la calle, sus actividades sociales, sus afiliaciones políticas, los periódicos y artículos concretos que lee, sus reacciones al respecto, los productos de su cesta de la compra, si sigue una alimentación sana, si su matrimonio es feliz, si mantiene relaciones extramatrimoniales, dónde se cita, cómo son sus relaciones

> privadas. Dado que hoy en día la mayoría de estas interacciones están mediadas de un modo u otro por los servicios de telecomunicación o por dispositivos móviles, nuestros proveedores de servicios de Internet guardan toda esa información, a la espera de que el gobierno acceda a ella.

En Occidente al menos tenemos la oportunidad de luchar para oponernos a algunas de las medidas más draconianas que las distintas ramas de los gobiernos intentan aplicar a la relación de la ciudadanía con la red.

Considerando la fuerza que la comunidad defensora de los derechos civiles tiene en Occidente y la intensa vigilancia a la que Rusia tiene sometida la red, sería de esperar que los delincuentes informáticos vieran en Rusia un entorno implacablemente hostil. Sin embargo, la Federación Rusa se ha convertido en una de las mecas mundiales de la delincuencia telemática. El número de actuaciones policiales es ridículo, y el de condenados alcanza apenas las dos cifras. Aunque nadie lo diga, todos saben la razón. Los delincuentes informáticos rusos son libres de clonar tarjetas de crédito, piratear cuentas corrientes y distribuir correo basura, siempre y cuando los destinatarios de sus ataques residan en Europa occidental y Estados Unidos. Si a un *hacker* ruso le diera por estafar a un compatriota, sería apresado e introducido en la parte posterior de un vehículo sin matrícula en menos de lo que se tarda en decir KGB.

A cambio, cómo no, cuando el Estado ruso requiere de los servicios de un *hacker* para perpetrar un ataque brutal contra un supuesto enemigo, al *hacker* más le vale cooperar.

El año 2007 significó el apogeo de una organización informal de empresas con sede en San Petersburgo conocida como Red Rusa de Negocios, o RRN. Esa misteriosa red ofrecía alojamiento a webs personales o corporativas, pero sobre todo era conocida por ser la número uno en alojamiento blindado. La particularidad de estas empresas consiste en que no se interesan por el contenido ni la finalidad de las webs de sus clientes. A cambio de unas cuotas altísimas, protegen sus páginas de cualquier intento de intrusión jurídica o digital.

La razón de ser de los alojamientos blindados no siempre es burlar la ley, pero a menudo los delincuentes y los piratas se sirven de ellos con ese fin. Por ejemplo, resultan prácticamente indispensables para las personas y grupos que se dedican a la distribución de pornografía infantil. De hecho, los departamentos de investigación de varias empresas de seguridad han descubierto que en los registros de RRN figuraban clientes de ese tipo.

Esta clase de alojamientos se han revelado vitales también para los distribuidores de correo basura, ya que para repartir miles de millones de anuncios dudosos y virus se necesitan sistemas seguros y con gran capacidad. Las estafas nigerianas 419, los medicamentos falsos, los famosos alargamientos de pene y muchos otros productos (reales o imaginarios) invaden el mundo gracias a los alojamientos blindados. Muchos correos basura esconden virus o enlaces a páginas infectadas que, al activarse, pueden convertir un equipo en un soldado más de un ejército *botnet*.

Entre 2006 y 2007, su época de mayor expansión, la Red Rusa de Negocios llegó a gestionar —según Spamhaus, la organización *antispam* de Cardiff— dos mil cuarenta y ocho direcciones de internet. Spamhaus clasificaba a RRN «entre los mayores emisores de correo basura del mundo» y la acusaba de dar cobijo a vastas «redes dedicadas a la pornografía infantil, al *malware*, al *phishing* y a la delincuencia informática».

La gran importancia de la RRN se debe a la rentabilidad de las empresas de alojamientos blindados, que llegan a cobrar a sus clientes seiscientos dólares mensuales o más. Una página legal pagaría una décima parte de ese precio.

Sin embargo, su papel secundario es el más interesante. Los ataques contra Estonia empezaron con una lluvia de millones de correos basura a las redes informáticas del gobierno estonio. Posteriormente, François Paget, que trabaja para McAfee, el gigante norteamericano de la seguridad informática, analizó el contenido de los correos y descubrió que eran idénticos a los modelos emitidos a través de la RRN. A eso hay que añadir las declaraciones de Andy Auld, jefe de inteligencia telemática de la Agencia contra el Crimen Organizado británica, quien aseguró que, trabajando sobre el terreno, la policía británica había averiguado que el funcionamiento de la RRN dependía en parte de los sobornos a la policía local y los jueces.

Cabe la posibilidad de que la RRN instigara los ataques contra Estonia, pero parece poco probable. Lo más probable es que percibiera dinero por provocarlos o que las autoridades consideraran su participación en ellos como un acto de patriotismo. La conexión entre un conglomerado de proveedores de servicios de internet de San Petersburgo especializados en actividades delictivas y los ataques informáticos contra Estonia constituye uno de los mayores interrogantes de la historia de la delincuencia telemática y la seguridad informática.

Existen en internet tres grandes «amenazas», que se manifiestan con distintas apariencias. La primera es la delincuencia informática. Su

manifestación básica es el tarjeteo, el robo de datos de tarjetas de crédito y su clonación con fines lucrativos, pero existen muchas otras estafas. Una de las más rentables, por ejemplo, es el llamado *scareware*, un método perfeccionado por una empresa ucraniana llamada Innovative Marketing. La compañía reclutó varias docenas de jóvenes de Kiev, la capital de Ucrania, la mayoría de los cuales creían estar colaborando con una *start-up* dedicada a la venta de productos de seguridad legales. Pero no era así.

La empresa se dedicaba a enviar falsos antivirus que, una vez instalados en un ordenador personal, abrían una ventana en el navegador en la que se alertaba al usuario de que su equipo había sido infectado por un virus. El aviso explicaba que el único modo de deshacerse del virus informático infiltrado en el disco duro y la memoria RAM era hacer clic en un enlace y comprar «Malware Destroyer 2009», por nombrar solo uno de sus incontables productos.

Tras descargar el programa (al precio de cuarenta euros), Innovative Marketing solicitaba que el usuario eliminase los programas antivirus existentes, por ejemplo Norton, e instalase su producto. Una vez instalado, el programa no hacía nada, era una aplicación vacía; la única diferencia era que desde entonces el equipo era vulnerable a todos los virus y que el usuario había pagado por hacerse con tan dudoso privilegio.

Uno de los investigadores de McAfee en Hamburgo, Dirk Kolberg, realizó un seguimiento de esa operación. Siguió la pista de esos falsos antivirus hasta su fuente en Asia oriental y descubrió que el administrador de los servidores de Innovative Marketing se había dejado abiertos unos cuantos puertos, de modo que Kolberg pudo colarse en el servidor y explorarlo a placer. Ahí averiguó algo extraordinario. Innovative Marketing estaba amasando tal fortuna que había tenido que habilitar tres centralitas —en inglés, alemán y francés— a fin de prestar asistencia a los usuarios que, perplejos, intentaban instalar sus inútiles productos. Gracias a los recibos hallados en el servidor, Kolberg supo que la estafa del *scareware* había generado ingresos por valor de varias decenas de millones de dólares, lo que lo convertía en uno de los ejemplos más ilustrativos de la delincuencia telemática.

Además del *scareware*, existen los fraudes de «inflar y tirar» (*pump-and-dump*): los *hackers* acceden a webs financieras e inflan, por vía digital, el precio de las acciones para después venderlas y provocar un derrumbe de los valores. Y los fraudes de nómina, en que los delincuentes piratean los ordenadores de una empresa para inscribir a empleados fantasma en la base

de datos de la plantilla. Los *hackers* les asignan sueldos reales, que de mes en mes perciben las llamadas «mulas financieras». A cambio de una modesta remuneración, las mulas ingresan el dinero en un banco alejado del lugar del delito.

De la misma manera que internet ofrece un sinfín de posibilidades creativas a quienes ejercen actividades legales, también los delincuentes dan rienda suelta a su fantasía en la red.

El segundo gran grupo de fechorías en la red es el del ciberespionaje industrial. Según el informe anual de amenazas publicado por el gigante de las telecomunicaciones estadounidense Verizon, esta categoría representa el treinta y cuatro por ciento de la actividad criminal y todo apunta a que es la más lucrativa. Los avances en tecnología de la comunicación facilitan el robo de secretos industriales. Hasta la popularización de los ordenadores, robar material implicaba irrumpir de forma física en una empresa o, si el hurto lo cometía un infiltrado, encontrar la manera de obtener y distribuir los datos buscados.

Hoy en día, esas dificultades han desaparecido: los ladrones industriales pueden piratear el sistema de una empresa y peinarlo en busca de proyectos, estrategias de mercado, nóminas o lo que sea que estén buscando, para después descargarlo. Antes de convertirse en el legendario Iceman, Max Vision trabajaba en la Costa Oeste como controlador de penetración, es decir que las empresas le pagaban por intentar introducirse en ellas. En una entrevista personal, vestido con el mono naranja que es el uniforme de la prisión, Vision me explicó que «en aquellos años, solo había una empresa a la que no pude acceder, una gran compañía farmacéutica estadounidense». Es comprensible: el valor de las empresas farmacéuticas reside en la investigación, y el robo de fórmulas para nuevos tratamientos puede acarrear pérdidas de cientos de millones de dólares y la caída del precio de sus acciones.

Vision tenía clavada la espina de no haber podido romper ese sistema. «Naturalmente, después ataqué con un *phishing* y a los cinco minutos ya estaba dentro, pero no es lo mismo». Lo que quiere decir con eso es que envió mensajes infectados a las direcciones de correo electrónico de la empresa y que, en cuestión de minutos, uno de los varios miles de empleados cayó en la trampa. Queda, pues, demostrado que por infranqueable que parezca una fortaleza digital, las amenazas a la seguridad son incontables.

De forma parecida, gracias a las facilidades para recabar y almacenar datos, hoy en día es mucho más fácil dar un golpe desde dentro en una

empresa. Como es sabido, Bradley Manning, el hombre acusado de haber robado los cables diplomáticos estadounidenses publicados más tarde en la web de Wikileaks, se las arregló para descargar todo el material en un CD disimulado como si fuera un álbum de *Lady* Gaga.

Se sabe asimismo que el Stuxnet —hasta la fecha el virus más sofisticado del mundo— debió de introducirse en su objetivo aparente, las plantas nucleares de Irán, gracias a que alguien (a sabiendas o no) infectó el sistema informático con un CD o un lápiz de memoria. Los sistemas operativos nucleares de Irán no están conectados a internet, pero no dejan de ser redes, y el hecho de que el Stuxnet lograra infectarlos demuestra que se hallaban dentro del alcance de un cuerpo profesional de inteligencia.

El Stuxnet simboliza de forma visible el tránsito hacia la tercera gran amenaza: la guerra informática. Es un virus tan complejo que los investigadores estiman que, de haberlo creado una sola persona, su desarrollo habría requerido varios años, lo cual significa que un equipo de ingenieros tuvo que trabajar en él durante un tiempo considerable. El crimen organizado no opera de esa manera. La única organización capaz de desarrollar el Stuxnet es un Estado capaz de dedicar abundantes recursos al diseño y producción de armas cibernéticas ofensivas y defensivas, lo cual no impide que quienquiera que produjera el Stuxnet tomara prestadas muchas técnicas y códigos informáticos de las decenas de miles de *hackers* de sombrero negro o gris que habitan el ciberespacio. Los *hackers* con mala fe alimentan la creatividad en todas las áreas del lado oscuro de la red. Tanto el ejército como el sector privado, la policía y las agencias de inteligencia adoptan al instante las herramientas que *crackers* y *hackers* desarrollan.

Cuando el Stuxnet se infiltró con éxito en el sistema de control de varias instalaciones nucleares de Irán, las autoridades admitieron que había provocado una avería de gran envergadura en el funcionamiento de una estación altamente sensible. El suceso podría haber provocado una explosión. Esto demuestra que los cataclismos augurados por los llamados guerreros informáticos ya no pertenecen tan solo al plano teórico. A pesar de la gravedad que tuvo en su momento, el ataque a Estonia fue una fiesta comparado con lo que presagia el Stuxnet.

A los guerreros informáticos se los conoce también como segurócratas informáticos; ellos son los profetas que anuncian que el cielo está a punto de desplomarse sobre nuestras cabezas. Uno de los más elocuentes es Richard Clarke, que en su libro *Cyber War* describe la situación siguiente:

> Cuando llegas a la sala de situación, el director de la Agencia de Sistemas de Información de Defensa te está esperando al otro lado del teléfono de seguridad.
>
> La FEMA, la Agencia Federal de Gestión de Emergencias, ha informado de importantes incendios en refinerías y de explosiones en Filadelfia y Houston, así como de la liberación de letales nubes de gas cloro en varias plantas químicas de Nueva Jersey y Delaware.
>
> El Centro Nacional para el Control del Tráfico Aéreo de Herndon, Virginia, ha sufrido una caída total de sus sistemas.

La mayoría de los segurócratas alegan que la única manera de evitar un Pearl Harbor digital o ciberapocalipsis es invirtiendo dinero en sus empresas y laboratorios de ideas con el fin de intensificar la investigación sobre el tema.

De hecho, eso ya está ocurriendo. Los sucesos de Estonia aceleraron el camino hacia la militarización del ciberespacio. La OTAN empezó por aceptar la creación del Centro de Excelencia para la Ciberdefensa Cooperativa, de majestuoso nombre, en Tallin en 2005. Pese a acoger con entusiasmo la idea de un ciberinstituto de operaciones bélicas, los Estados miembros se mostraron reticentes a poner dinero sobre la mesa (con la comprensible excepción del país anfitrión, Estonia). El proyecto no quedó archivado, pero encontró dificultades para avanzar mucho más allá del estadio de texto impreso en papel con membrete de diseño.

«Nada más producirse el ataque —explica Peeter Lorents, eminente matemático estonio y uno de los fundadores del centro—, la atmósfera cambió y comenzamos a recibir ayuda de Bruselas y Washington. De hecho, mi primera reacción al saber del ataque fue telefonear a Francia y pedir dos cajas de champán Cristal para el señor Putin. Con ese ataque, los rusos habían garantizado el futuro de nuestro centro».

En Washington sin duda sonaban ya todas las alarmas. Varios sucesos ocurridos inmediatamente antes o después del incidente estonio convencieron en 2009 a la entrante administración Obama de que era necesario mejorar la ciberdefensa a toda costa. Poco después de los sucesos de Estonia, uno de los más importantes organismos de vigilancia global de Estados Unidos, la Agencia Nacional de Seguridad (NSA), se dio cuenta de lo grave que había sido la pérdida de un avión de reconocimiento EP-3E Aries que, en abril de 2001, cayó en manos de las fuerzas aéreas chinas. El piloto había conseguido destruir todos los programas antes de estrellarse, pero el *hardware* estaba intacto y, nada más caer en manos de los chinos, estos sometieron su

avanzada tecnología a un proceso de ingeniería inversa que habría de permitirles localizar y descodificar comunicaciones encriptadas. Poco después de la entrada de Obama en la Casa Blanca, China empezó a probar su nuevo juguete y la NSA detectó que el país disponía de nuevos instrumentos para interceptar comunicaciones. Por lo visto, China quería hacerle saber a Washington que había conseguido piratear con éxito su tecnología.

El gobierno de Estados Unidos no se conformó con prestar su apoyo al centro de ciberdefensa de Tallin, que desde 2008 lleva a cabo proyectos de alta investigación, entre ellos complejas maniobras militares cibernéticas. Las redes informáticas habían adquirido tal importancia tanto para la estructura del Departamento de Defensa como para su capacidad ofensiva y defensiva que Robert Gates, el secretario de Defensa, tomó la trascendental decisión de crear una nueva rama militar: el ciberespacio.

Esta quinta rama —hermana de las de tierra, mar, aire y espacio— es la primera esfera de operaciones militares creada por el hombre y las reglas de combate por las que se rige resultan de una opacidad casi absoluta. Además de esta rama militar, el Pentágono había creado el Cibercomando con el propósito de prevenir actividades hostiles en el ciberespacio y, en caso necesario, echar mano de armas ofensivas como el Stuxnet. Por el momento, Estados Unidos es reconocido como el país líder en cibercapacidad ofensiva.

No debe confundirse la expresión «cibercapacidad ofensiva» con la posibilidad de emplear armas convencionales controladas por sistemas informáticos. El mejor ejemplo de este segundo tipo de arsenal son los vehículos no tripulados (utilizados de forma regular por Estados Unidos en Afganistán y en Pakistán), capaces de llevar a cabo misiones de vigilancia y combate bajo el pilotaje de un especialista en Nevada.

Las armas informáticas son herramientas de pirateo mediante las cuales un soldado informático penetra en los sistemas de una ICN (infraestructura crítica nacional) enemiga, como por ejemplo sus redes energéticas o de suministro de agua. Una vez obtenido el control del sistema, el cibercomandante puede ordenar su paralización (o, como sabemos en el caso del Stuxnet, desencadenar una peligrosa serie de explosiones), de tal modo que, en cuestión de días, la comunidad afectada puede experimentar una regresión tecnológica a la Edad de Piedra.

Al menos en teoría. Por el momento, Estados Unidos es pionero en el desarrollo de armas informáticas, si bien China, Francia e Israel le pisan los talones, a no mucha distancia de la India y Gran Bretaña.

La militarización del ciberespacio era previsible; lo que nadie sabe es adónde puede conducirnos. En un artículo aparecido en *The New Yorker,* el sagaz Seymour Hersh analizaba las consecuencias de que China se hubiera apropiado de los secretos ocultos en el disco duro del avión de reconocimiento:

> La debacle del EP-3E alimentó un largo debate en el ejército y en la administración Obama. Muchos líderes militares interpretan la respuesta de China como una advertencia sobre vulnerabilidades presentes y futuras, sobre la posibilidad de que China, o cualquier otro Estado, pueda utilizar sus crecientes habilidades cibernéticas para atacar infraestructuras civiles y complejos militares en Estados Unidos. Frente a estos, están quienes abogan por una respuesta civil a la amenaza, centrada en la difusión del uso del encriptado. Su temor es que un exceso de confianza en la voluntad del ejército pueda tener consecuencias adversas para la privacidad y las libertades civiles.

Todo apunta a que la tendencia será designar al ejército como árbitro supremo en el campo de la ciberseguridad. En octubre de 2010, el presidente Obama encomendó a la Agencia de Seguridad Nacional —parte del Pentágono— que colaborase con el Departamento de Seguridad Nacional y el sector privado en las tareas de seguridad cibernética del país. En China, el Ejército Popular de Liberación es la principal institución encargada de velar por la seguridad cibernética interior y exterior, mientras que en Oriente Próximo las Fuerzas de Defensa israelíes son fuente de inspiración de extraordinarias investigaciones realizadas en el campo de la guerra informática, cosa que permite a Israel enfrentarse a rivales mucho más poderosos que él en este terreno.

Llegados a este punto, alguien podría preguntarse, y con razón, qué relación guarda todo esto con la delincuencia informática.

Las amenazas del ciberespacio son reales y peligrosas. En un mundo ideal, un Estado democrático velaría para que esta tecnología fundamental mejorara la vida de sus ciudadanos sin causarles perjuicios. De igual modo, el Estado no debería ceder a la tentación de atropellar nuestros derechos e intimidad. Permitir que el ejército asuma un papel preponderante en la defensa de las redes civiles supone un yerro garrafal. Pero, puesto que las armas informáticas tienen potencial para paralizar las infraestructuras críticas

de un país (y destrozar de paso la vida de sus habitantes), debe contemplarse la intervención del ejército en casos de emergencia. Dichos casos deben tener carácter excepcional y verificable.

La responsabilidad de supervisar las distintas clases de amenazas —delincuencia informática, ciberespionaje industrial y guerra informática— debe recaer sobre organismos diferentes. Los cuerpos policiales reconocidos, como el FBI o el Servicio Secreto, tendrían que hacerse cargo de la delincuencia telemática; las empresas y compañías deberían desarrollar sus propios sistemas de ciberseguridad o contratar los servicios de empresas especializadas; en cuanto al gobierno civil, debería contar con su propia red de defensa, en tanto que el ejército tendría que proteger sus propios sistemas.

A primera vista parece bastante sencillo. Pero en la vida real los compartimentos se solapan, debido, entre otras cosas, a las interconexiones de la red. Además, a día de hoy desconocemos la respuesta al gran enigma de la ciberseguridad: ¿cómo reconocer un ciberataque?

Para responder a ello, un ciberdefensor necesita conocer dos datos vitales: la procedencia del ataque y la motivación del atacante. Cuando el atacante es un profesional, ni siquiera el mejor defensor es capaz de hallar respuestas. A lo sumo, puede barajar hipótesis, que —al no ser más que suposiciones— pueden desembocar en decisiones erróneas, malentendidos y, en última instancia, conflictos.

Imaginemos que los cuerpos policiales, el sector industrial y el ejército se ciñen a su tarea de proteger al Estado contra los peligros arriba citados. Siguen quedando dos actores, siempre presentes sea cual sea el tipo de amenaza: el policía infiltrado y el *hacker*. El primero intenta hallar la solución del enigma (aunque no necesariamente para compartir sus hallazgos); el segundo se encarga de formular el enigma de tal manera que resulte insoluble.

Las agencias de inteligencia rastrean la red como un gato negro sobre un fondo oscuro, con sigilo y relacionándose solo cuando de lo que se trata es de fingir, ganar adeptos o sembrar confusión. Ese fantasmal modo de proceder forma parte de los genes de los agentes infiltrados, pero también se explica por la fascinación, admiración incluso, que los servicios de inteligencia sienten hacia sus principales enemigos en el ciberespacio: los *hackers*.

Hasta hace poco, los defensores de la red daban por hecho que los *hackers* eran los cerebros de todos los ataques que se producían. Esto ha cambiado en los últimos cinco años con la aparición del *malware* «comercial». Hoy en día, muchos *hackers* ya no se ganan la vida pirateando tarjetas de crédito y cuentas corrientes o por medio de otras astucias, sino que se dedican

simplemente al desarrollo y la venta de troyanos, virus y gusanos. Se trata de programas sencillos que no requieren conocimientos especializados por parte del usuario. Su forma más habitual es el *botnet*. Los *hackers* arriendan *botnets* para lanzar ataques DDoS destinados a fines tales como extorsiones o venganzas durante un par de días, como mucho una semana o un mes. Como es natural, los *hackers* que venden *botnets* y virus poseen la habilidad técnica necesaria para controlar la duración del arriendo y los programan con fecha de caducidad; superada esta, los clientes —casi siempre delincuentes de tres al cuarto— dejan de poder utilizar el producto.

Con todo, la aparición en la red de un mercado secundario de *malware* comercial no altera la verdad fundamental de que detrás de cada ataque informático —ya sea con fines de hurto, de espionaje industrial o bélicos— se esconde un *hacker* profesional. Para la elaboración de un ciberataque de veras dañino, y no simplemente molesto, resulta indispensable poseer grandes conocimientos técnicos. Esto significa que, aunque trabaje por cuenta de otra persona (trátese de un capo, un consejero delegado o un comandante), el *hacker* debe conocer en profundidad el objetivo establecido, si lo que pretende es diseñar un producto adecuado. Fuera cual fuese el equipo de *hackers* que diseñó el Stuxnet, por ejemplo, debía de estar familiarizado no solo con las plantas nucleares iraníes marcadas como objetivo, sino también con la red Siemens PLC que las gestionaba y con el tipo exacto de compresor diseñado por Vachon, una empresa finlandesa (aunque fabrica en China), así como con la empresa taiwanesa RealTek, cuyo certificado digital fue pirateado con el fin de engañar al programa antivirus del sistema iraní. Quienquiera que haya diseñado el Stuxnet sabía muy bien que debía elegir con cuidado a su víctima.

En este sentido, los *hackers* son el elemento clave en la ciberseguridad, ya que conocen la solución del enigma. Dar con el *hacker* es el primer paso hacia la verdad.

La abrumadora cantidad de recursos que los gobiernos dedican hoy en día a la ciberseguridad se invierte en «soluciones digitales», es decir, en combatir unos inventos con otros. Los fondos dedicados a comprender a los *hackers*, su cultura, su forma de pensar, sus intenciones y sus vulnerabilidades son insignificantes. Claro que no es fácil encontrar a un *hacker*. ¿Cómo saber, en internet, si la persona a la que acabamos de conocer es un *hacker*, un espía de la policía, un agente de inteligencia, un investigador de las fuerzas aéreas, un bromista, un terrorista o un extraterrestre?

La confianza es el quid del asunto, y para ganarse la confianza de otros hay que ser paciente y cultivar las relaciones. Sin embargo, el tiempo es un bien escaso en el mundo de la seguridad informática. Nada refleja mejor las dificultades relativas a la confianza y al tiempo que el alejamiento de Dark Market de sus países de origen —Gran Bretaña, Alemania y Estados Unidos — y su traslado a un país cuya importancia económica y geoestratégica aumenta a pasos agigantados: Turquía.

LIBRO SEGUNDO

PARTE I

26

BILAL EN PITTSBURGH

Pittsburgh, Pensilvania, febrero de 2008

Era una fría y despejada mañana de invierno de 2008, y el inspector Bilal Şen, de la policía turca, echó un vistazo a través de la ventana de su despacho en dirección al puente Hot Metal de Pittsburgh. El puente cruza el río Monongahela ligeramente al este de su confluencia con el Allegheny, con el cual forma el majestuoso río Ohio, y en tiempos era utilizado para transportar metal fundido desde los altos hornos de Eliza, al norte, hasta los molinos de laminación del sur.

Pero ese día no había tiempo para pensar en la nevada estética posindustrial de Pittsburgh. Acababa de leer algo inquietante en el foro de Dark Market. A juzgar por las noticias, a todas luces fiables, llegadas de Estambul, Cha0, el delincuente informático al que investigaba el inspector Şen, era «un pez gordo, rico y poderoso». Para un turco, aquella frase era fácil de descifrar: quería decir que el objetivo tenía amigos en las altas esferas, la peor pesadilla para un policía turco.

El inspector Şen llevaba casi tres meses trabajando en la Alianza Nacional para la Formación en Informática Forense. El primer día estaba esperando en la recepción a ser recibido por el jefe de la organización cuando, por azar, apareció el agente Keith J. Mularski, radiante y encantador como de costumbre. Se presentó y, al saber que Bilal era turco, empezó a explicarle todo lo que sabía sobre Cha0, el famoso administrador y maestro criminal de Dark Market. Mularski y Şen hicieron buenas migas desde el principio.

Nada más entrar en la zona de despachos del cuarto piso del 2000 de Technology Drive, el policía turco contempló extrañado la apariencia del lugar, que recordaba más a una empresa de seguros que al frenético entorno tecnológico de series televisivas como *CSI Nueva York*. Al fondo había una sala donde podían encontrarse todas las herramientas necesarias para el ejercicio de la investigación forense, máquinas que sirven en bandeja los secretos más recónditos de cualquier aparato digital. Pero esa sala era apenas

visible y se hallaba sellada para evitar que los objetos sometidos a examen pudieran ser contaminados por troyanos o *malware* (como sus equivalentes orgánicos, a veces los virus informáticos se transmiten por el aire). Aparte de eso, el recinto era un lugar tranquilo, ordenado y de lo más corriente.

Esa primera mañana, Keith le mostró a Bilal la pizarra blanca de su despacho, donde el nombre de «Cha0» aparecía en lo alto de una pirámide de delincuentes vinculados a Dark Market. El agente turco sintió una punzada de vergüenza en su interior. Seis meses antes, y con la ayuda de sus compañeros británicos y alemanes, los federales habían hecho caer a JiLsi y Matrix, dos de los administradores más activos de Dark Market. Se habían practicado detenciones en Gran Bretaña, Alemania, Canadá y Francia, y se preparaban más en Estados Unidos. De aquí que el agente de Ankara considerase una mancha en su orgullo nacional, así como en su reputación personal, que un paisano suyo se contara entre los delincuentes informáticos más buscados del mundo entero.

La policía turca, y en concreto el departamento contra el crimen organizado, había hecho grandes progresos a lo largo de la década anterior, y Bilal estaba decidido a demostrar que, aunque sus recursos fueran muy inferiores a los de sus colegas de Europa occidental y Norteamérica, la joven Unidad contra el Crimen Cibernético con sede en Ankara, la capital turca, era capaz de jugar en primera división.

Agentes de policía de todo el mundo entraban y salían a todas horas de las oficinas del FBI. Viajan ahí para aprender de sus colegas estadounidenses, pero también para crear redes de asistencia mutua. La colaboración entre cuerpos de policía de distintos países se resentía a menudo de los interminables trámites burocráticos, y la amistad personal entre los agentes era la forma más rápida de esquivarla.

A Bilal se le había concedido una estancia de tres meses. Para los federales, el turco representaba un contacto nuevo y potencialmente muy útil. En 2003 había sido uno de los dos fundadores de la pequeña Unidad contra el Crimen Cibernético, adscrita a la División contra el Contrabando y el Crimen Organizado. En comparación con los recursos de los delincuentes a quienes perseguía, los del inspector eran precarios.

Bilal Şen estaba deseoso de aprender del FBI. No porque no tuviera experiencia; de hecho, había entrado en la policía a los quince años, en 1989, año en que firmó su acceso al extenuante curso de adiestramiento de agentes, el más largo del mundo, de ocho años de duración. Curiosamente, dada su escasa estatura y su aspecto meditabundo, el inspector Şen recordaba más a

un Hércules Poirot en versión turca que a la imagen arquetípica del duro policía balcánico curtido a base de enfrentamientos con bandidos rurales, cárteles urbanos de la droga y la indiferencia del sistema penal.

El cuerpo de policía imponía un régimen severo, pero lo que más le dolió a Bilal no fueron ni la austeridad de los cuarteles ni los extenuantes cursos de asalto, sino la total ausencia de ordenadores. Desde muy joven había aprovechado la menor ocasión para escaparse a la sala de videojuegos de su ciudad natal de Eskişehir, a medio camino entre Estambul y Ankara, en la mitad norte de Anatolia. Tendría unos seis años cuando descubrió un juego llamado *River Raid*. El muchacho dedicaba todo su tiempo libre a pilotar un caza bidimensional con el que recorría un río abriendo fuego contra pequeños helicópteros, barcos, tanques y dirigibles, procurando, al mismo tiempo, repostar combustible. Atrapado por aquella misteriosa mezcla de repetición y recompensa ocasional que impide a tantos niños, adolescentes y jóvenes adultos despegarse de las pantallas de sus ordenadores, Bilal sentía por los videojuegos una obsesión semejante a la de muchos *protohackers* a esa misma edad. Como ellos, estaba dispuesto a todo con tal de vencer a la máquina.

Fue quizá esa tozudez lo que ayudó al bisoño recluta a soportar su primer destino en una comisaría de pueblo en el lugar más perdido de Anatolia. Corrían los años noventa, pero allí la tecnología se reducía a una vieja máquina de escribir mecánica. Levantar acta de las declaraciones de testimonios se consideraba indigno de su cargo como agente, pero Bilal quería mejorar su mecanografía y pasaba horas y horas aporreando las teclas. El resto del tiempo, aquel prodigioso autodidacta se dedicaba a estudiar mandarín.

Cuando solicitó entrar en la Unidad contra el Crimen Organizado, un cuerpo de élite, su superior le preguntó por qué estudiaba chino. «Ahora que China abrirá sus puertas al exterior —respondió—, el Departamento contra el Crimen Organizado necesitará hablantes de mandarín». La respuesta fue un éxito y se hizo con el puesto.

Ya en la capital turca, el joven detective se matriculó en un máster en la Universidad de Ankara que pagó de su bolsillo y cursó durante sus horas libres. Escogió un tema desconocido en Turquía, «Oportunidades y riesgos del gobierno electrónico», que le permitió estudiar la relación entre privacidad, derechos civiles y delincuencia informática.

Bilal Şen empezó a investigar la proliferación de la delincuencia telemática en su país. Pocos eran los agentes turcos capaces de hacerlo; los

únicos cuerpos del Estado concienciados de la importancia estratégica de la seguridad informática eran el ejército y las agencias de inteligencia. Pero, como es natural, estos no facilitaban información ni sobre su capacidad operativa ni sobre sus actuaciones.

Con la ayuda de un compañero, Bilal hizo suya la hercúlea tarea de persuadir al rígido Ministerio del Interior de que destinase parte de sus codiciados fondos a la creación de una Unidad contra el Crimen Cibernético. Fueron necesarios tres años de súplicas, adulaciones y politiqueos. Por suerte, contaba con un colaborador experto en el arte otomano de caer en gracia a los burócratas del Ministerio del Interior.

Como todas las unidades dedicadas a la delincuencia cibernética surgidas en los distintos cuerpos de policía del mundo, el nuevo departamento turco podía aprovecharse de la circunstancia de que prácticamente nadie entendía cómo funcionaba el lado oscuro de la informática. Una vez obtenido el visto bueno, los dos agentes gozaron de una libertad nunca vista, sin interferencias de ninguna clase, ya que nadie tenía la más mínima idea de cuál era su trabajo y no suponían ninguna carga para el erario.

A diferencia del propio gobierno del inspector, que apenas si sabía en qué se ocupaba, sus colegas del otro lado del Atlántico no tardaron en tomar nota de sus logros. En el verano de 2007, mientras las policías de Alemania y Gran Bretaña arrestaban a Matrix001 y JiLsi, los administradores de Dark Market, el equipo contra la delincuencia informática turco ponía entre rejas a Maksik, uno de los ciberdelincuentes más importantes. Miembro destacado de Dark Market (se encargaba, entre otras cosas, de proporcionar *dumps* al *hacker* marsellés Lord Kaisersose), Maksim Yastremski, nativo de Járkov, en el noreste de Ucrania, había dado por hecho que en Turquía se hallaría seguro, no solo porque no se había arrestado a ningún delincuente informático en el país, sino porque las relaciones entre Ucrania y Turquía nunca habían sido mejores, sobre todo en los círculos del hampa.

Los ucranianos, además, adoraban Turquía por su fabulosa costa; las deliciosas playas de Antalya eran destino obligado para los ciberladrones de ambos países.

El Servicio Secreto estadounidense llevaba dos años tras los pasos de Maksik. En 2006, habían logrado acceder a su portátil y posteriormente habían concertado varias reuniones entre él y un agente encubierto en Tailandia, Dubái y Turquía. Hasta entonces, la colaboración con Turquía había sido difícil, cuando no imposible, pero con la detención de Maksik bajo el tórrido sol de Antalya, la policía turca había dado a entender que no solo

estaba dispuesta a colaborar en materia de delincuencia informática, sino que sabía cómo hacerlo.

A pesar de que JiLsi y Matrix habían desaparecido de los foros, el resto del grupo seguía activo; de hecho, Dark Market estaba experimentando un nuevo aumento de su actividad. Irónicamente, la clave de aquel resurgimiento se hallaba en la detención de otro delincuente: Iceman.

En septiembre de 2007, la policía estadounidense había conseguido por fin localizar a Max Vision en su escondite del centro de San Francisco. Con la desaparición de Iceman, Carders Market se había desmoronado, de modo que, en tanto que Mazafaka se hacía con el control del mercado de tarjetas ruso, Dark Market se convertía en líder indiscutido de la ciberdelincuencia en lengua inglesa. Directa o indirectamente, la página seguía generando cada mes cientos de miles de libras en dividendos ilegales y su popularidad entre tarjeteros y *hackers* seguía siendo tan grande como siempre.

Quedaban en Dark Market tres actores principales: Cha0, Master Splyntr y Shtirlitz. Pronto se les uniría el misterioso Lord Cyric. La presencia de Lord Cyric suscitaba antipatía y devoción a partes iguales entre los tarjeteros. Quienes lo aborrecían creían que era Mularski, el topo del FBI, aunque también circulaban sospechas de que Master Splyntr y Shtirlitz podían estar trabajando para o con las fuerzas de seguridad estadounidenses. En lo que todo el mundo, tanto *hackers* como agentes, estaba de acuerdo era en que Cha0 era el más peligroso de los que quedaban.

A diferencia de las abultadas carpetas relativas a sus compañeros de Dark Market, Mularski y Şen conocían tan solo dos datos destacables acerca de Cha0: que vivía en Estambul y que dirigía un próspero negocio dedicado a la venta de clonadoras, instrumentos indispensables para cualquier estafador de la Edad del Plástico. Sin embargo, no disponían ni de un nombre real, ni de una dirección física, ni de una dirección IP, ni de socios conocidos. O bien Cha0 no existía (lo cual no era imposible), o bien jamás había cometido ningún error.

Si se trataba de lo segundo, podía ser que Cha0 hubiera perfeccionado un sistema para no dejar huellas digitales, impidiendo con ello que los sabuesos forenses pudieran dar con su paradero. El responsable de parte de ese sistema de enmascaramiento era Grendel, que en sus ratos libres prestaba ayuda (remunerada) a Dark Market. Cosa irónica, ya que Grendel proporcionaba también los *shells* que ocultaban la localización de los servidores de Mularski. Grendel, que en la vida real trabajaba para una empresa de seguridad aplicada a las tecnologías de la información en Alemania, facilitaba sus servicios a

Dark Market por invitación de JiLsi. Resulta contradictorio, pero muy característico de Dark Market, que terminara ofreciendo seguridad tanto a los delincuentes como a los policías de la web.

A pesar de sus esfuerzos, Bilal Şen no había conseguido relacionar el estilo (o *modus operandi*, como lo llama la policía) de Cha0 con el de ninguno de los delincuentes conocidos en Turquía. Parecía reunir las dos características fundamentales de quienes frecuentan el lado oscuro de internet: poseía habilidades técnicas prodigiosas y, a la vez, era un delincuente profesional que cuidaba todos los detalles y no dejaba nada al azar. Incluso cabía la posibilidad de que Cha0 fuera el nombre colectivo de una organización bien regulada, aunque los análisis lingüísticos sugerían que los mensajes que colgaba en la red eran obra de una sola persona.

Por eso, cuando Bilal fue advertido desde Estambul de que Cha0 era «un pez gordo», no solo se preocupó, sino que supo que en el futuro, y a pesar de la gran velocidad a que estaba modernizándose su país, tendría que actuar con tacto.

Con el cambio de milenio, Turquía se había convertido en un destino cada vez más popular entre *hackers*, *crackers* y delincuentes informáticos. A finales de la década de 1990, buena parte de las actividades ilícitas de internet se realizaban desde ciertas regiones de los llamados países BRIC. Un economista de Goldman Sachs había denominado con esas siglas a Brasil, Rusia, la India y China por ser los países líderes de los mercados emergentes y el segundo grupo de poder global por detrás del G8 (si bien Rusia forma parte de ambos).

Los BRIC compartían importantes características sociales y económicas. Poseían economías dinámicas y en proceso de apertura tras varias décadas de estancamiento; eran países con un gran número de habitantes y con políticas que, combinadas, se traducían en una elevada tasa de crecimiento; al mismo tiempo, su transformación en actores globales dinámicos iba acompañada de un exuberante, y en ocasiones agresivo, nacionalismo. Sus sistemas educativos ofrecían una formación básica excelente que, unida a las flagrantes desigualdades en el reparto de la riqueza, habían generado una nueva clase de jóvenes pobres y sin empleo, pero —a diferencia de generaciones anteriores — con grandes aspiraciones materiales fomentadas por los mensajes consumistas inherentes a la globalización. Con el fin de satisfacer dichas aspiraciones, una minoría empezó a frecuentar las cafeterías de internet, a salvo de la vigilancia policial o de cualquier otro tipo, donde encontraron mil maneras para formarse en el arte de los *hackers*.

Turquía figuraba como miembro honorífico de los BRIC, con una economía que comparada, por ejemplo, con la de Rusia, parecía mucho más dinámica. Su población, de unos dieciocho millones, y sus tasas de crecimiento aumentaban a mayor velocidad incluso que las de los BRIC. Todo el mundo reconocía su importancia estratégica: con su acceso al mar Negro y al Mediterráneo y sus fronteras compartidas con Bulgaria, Grecia, Irán, Irak, Siria y Armenia, países que en las últimas dos décadas habían vivido agitaciones o guerras de un tipo u otro. La política turca siempre ha sido imprevisible. Pero, con el cambio de milenio, el floreciente poder económico del país y su creciente sofisticación le concedieron un papel protagonista en varias regiones geoestratégicas: Oriente Próximo, Asia central, el mar Negro y los Balcanes.

El desarrollo de la infraestructura de internet del país fue lento durante la década de 1990, pero en los últimos años se ha puesto al día rápidamente. Estambul, el motor económico de Turquía, vivió un estallido de *start-ups* de éxito y muchas compañías de diseño, medios de comunicación y servicios se beneficiaron de ello.

El inconveniente era que el tamaño del país, sus crecientes infraestructuras y la generalización de la instrucción juvenil en las clases medias eran caldo de cultivo para la delincuencia informática. Hasta la entrada en funcionamiento, en 2005, de la unidad de Bilal Şen, apenas existían medidas destinadas a impedir que *crackers* y *hackers* operaran en la red desde Turquía sin miedo a ser detectados. Con la Unidad contra el Crimen Cibernético las cosas empezaron a cambiar, pero las dificultades eran constantes. Si el inspector Şen lograba dar con Cha0, la unidad podría colgarse una importante medalla.

Sin embargo, poco antes de regresar a Turquía desde Pittsburgh a mediados de marzo de 2008, el inspector recibió una noticia que complicaba aún más la investigación. Sus contactos de Estambul le comunicaban los detalles de una desconcertante entrevista concedida a Haber 7, una famosa agencia de noticias, por parte de un *hacker* turco llamado Kier, que confesaba ser un fugitivo de la ley.

La reputación de Haber 7 se basaba en parte en el apoyo espiritual que recibía de un importante movimiento islamista turco conocido como la Comunidad Gülen, dedicado a promover la filosofía de su líder, Fethullah Gülen, exiliado en Estados Unidos. En tanto que agencia de noticias de la Comunidad, Haber 7 se mostraba abiertamente favorable al partido en el poder, el AKP, proislámico y demócrata.

El joven Kier había declarado a la agencia de noticias que no solo conocía a Cha0, sino que la persona, o personas, escudada tras el más conocido de los misteriosos avatares de Dark Market planeaba expandir su imperio criminal. El artículo incluía una fotografía del *hacker* conversando en una cafetería de Estambul. La imagen estaba tomada de espaldas, pero parte de su perfil era visible.

Por entonces, Bilal no sabía todavía que aquel *hacker* era un joven llamado Mert Ortaç, un personaje de lo más peculiar de quien se sospechaba que pudiera ser cómplice de otro delincuente llamado Cryptos, detenido en enero de 2008 bajo la acusación de haber atacado a Akbank, una de las mayores instituciones financieras de Turquía. En cierto modo, el caso de Akbank tenía mayor calado que el de Dark Market, ya que el pirata habría irrumpido en el sistema central del banco aprovechándose de una vulnerabilidad de su sistema operativo. Sin embargo, ni la policía de Estambul ni la División contra el Crimen Organizado tenían la menor idea de cuál podía ser el escondite de Ortaç. Y de repente, ahí estaba, charlando con un periodista.

Pese al hostigamiento de la policía de Estambul y de un equipo de agentes de inteligencia, Ortaç explicó al reportero que en diciembre de 2007 les había dado esquinazo y se había pasado a la clandestinidad, de donde solo había salido para conceder aquellas extrañas y fragmentarias declaraciones.

La entrevista ponía en evidencia a la policía de Estambul. La facilidad con que el delincuente había evitado ser capturado despertaba inquietud. Para acabarlo de arreglar, el *hacker* advertía que las detenciones por el caso Akbank no tendrían efectos en la seguridad de los bancos turcos, ya que otro delincuente, aún más peligroso, se hallaba en proceso de sustraerles hasta el último centavo posible, y su nombre era Cha0. (Por supuesto, Bilal Şen sabía de la existencia de Cha0, pero era la primera vez que oía su nombre en público y en boca de alguien tan misterioso).

Ortaç aseguraba también que Cha0 gozaba de la protección de funcionarios del gobierno. Por lo menos, la entrevista venía a confirmar que Cha0 era de verdad. Pero eso no impidió que, al leerla, Şen sintiera abrirse el suelo bajo sus pies. ¿Quién podía estar protegiendo a Cha0? ¿Y por qué?

27

EL PORTAL SUBLIME

El inspector Şen levantó la vista de sus notas y sintió que su inquietud empezaba a convertirse en miedo. Acababa de saberse que Cha0 había enviado un mensaje al canal de noticias Haber 7 en respuesta a la entrevista con Ortaç. El escrito era una diatriba sazonada con pizcas de megalomanía y de una férrea convicción: «Yo soy el último representante de la ley en Dark Market —clamaba—. Evito la intrusión de policías y *rippers*. Dicto las reglas y todo el mundo obedece».

Los contactos del inspector sugerían que posiblemente Cha0 estaba más allá del alcance de la ley. Şen habló con un viejo amigo de la policía de Estambul. El caso era preocupante: ambos temían que Cha0 contara con un topo en el cuerpo que lo mantuviera al corriente de los avances de la investigación. Si no podían confiar en su equipo, en su apoyo y, sobre todo, en sus superiores, ¿cómo iban a resolver el caso?

En la entrevista, Mert Ortaç había hablado por extensión sobre la policía secreta y otras fuerzas relacionadas con el caso de Dark Market. En algunos países, aquello habría olido a teoría de la conspiración, pero tratándose de Turquía no podía descartarse que fuera cierto. Mert había dejado entrever que la operación de Dark Market podía salpicar a nombres de la élite económica, militar y política.

La compleja estructura política del país se había redefinido desde que en las elecciones de 2002 el AKP se convirtiera en la fuerza política dominante. Teniendo en cuenta que el 90 por ciento de los turcos son musulmanes, que un partido declaradamente islámico hubiera ganado por mayoría no era en sí motivo de sorpresa. El AKP insistía en que su fe religiosa estaba subordinada a su compromiso democrático, de igual modo que muchos partidos conservadores europeos que se definen a sí mismos como democristianos.

Pero Turquía tenía a gala provenir de otra fuerte tradición ideológica: el kemalismo. Bautizada en honor al fundador de la Turquía moderna, Kemal Atatürk, su principio rector promovía la completa separación entre Iglesia y Estado. La ubicua presencia de la imagen de Atatürk en tiendas, hogares,

despachos, cuarteles, hospitales y prisiones reflejaba la profunda admiración que despertaba el laicismo de su legado entre los turcos (así como el miedo a ser detenidos por desacato).

Del kemalismo, no obstante, existen interpretaciones para todos los gustos. Sus dos defensores más acérrimos provienen de la élite laica de clase media: intelectuales, profesionales liberales y funcionarios, por un lado, y el llamado Estado Profundo, por el otro. El recelo entre ambos, y hacia el AKP, es considerable.

La de Estado Profundo es una denominación significativamente siniestra que designa al complejo militar-industrial que ejerció un arbitraje decisivo en la política turca en el periodo de la posguerra. Al ser uno de los dos únicos miembros de la OTAN con frontera con la Unión Soviética (el otro era Noruega), Turquía desempeñó un papel clave durante la guerra fría, y sus aliados, Estados Unidos el primero, miraron hacia otro lado ante los flagrantes abusos que el ejército cometía contra la población.

Las continuas interferencias de los servicios de seguridad en la vida política turca dejaron secuelas también en la economía del país, hasta el punto de que en ocasiones se hacía difícil distinguir entre el depredador y la presa. El Estado Profundo defendía aquel complicado y lucrativo estado de cosas apelando al kemalismo: si consideraba que el frágil orden democrático ponía en riesgo sus intereses económicos, el ejército intervenía con la excusa de proteger el legado de Atatürk. Tradicionalmente, las fuerzas armadas no toleraban que nadie les saliera al paso. Parafraseando un viejo dicho turco: «Dale la mano al Estado Profundo y te arrancará el brazo».

Sin embargo, en los últimos quince años los sucesivos gobiernos turcos han acometido una serie de reformas, en parte para cumplir con los requisitos de admisión en la Unión Europea. Pese a las voces temerosas de que pudieran tener oculto un programa islamista radical, los nuevos mandatarios del AKP han impulsado cambios de corte netamente liberal en la sociedad turca, como por ejemplo la abolición de la pena de muerte. Otra muestra de consolidación del Estado de derecho ha sido la promoción por parte del AKP de la separación entre las fuerzas policiales y el ejército.

Este proceso ha tenido como consecuencia cambios notables y muy positivos. Algunos sectores del funcionariado han comenzado a comprender que su cometido principal no consiste en blindar sus privilegios, sino en prestar servicios al ciudadano de a pie, y que, si el Estado turco funciona de forma eficaz, su influencia y consideración crecen en el plano internacional.

Pero el lento nacimiento de la nueva Turquía no ha sido un proceso indoloro ni sus frutos han sido siempre los esperados, sino que ha ido acompañado de titánicas luchas políticas en las que las cambiantes alianzas entre fuerzas oscuras se han revelado letales para todo aquel que, a sabiendas o por ignorancia, se interpusiera en su camino.

El principal teatro de operaciones de la guerra entre esas fuerzas se inauguró de forma oficial en 2007, con la apertura de la llamada investigación Ergenekon. Ergenekon, cuyo nombre alude a una antigua leyenda épica turca, fue como se denominó a una supuesta conspiración del Estado Profundo en la que líderes militares, políticos y de los servicios de inteligencia habrían colaborado con miembros del crimen organizado, periodistas, abogados y otros profesionales liberales. Su objetivo habría sido restringir la influencia de los gobiernos elegidos por vía democrática, en especial el AKP. No solo eso, sino que, según la fiscalía y los medios más afines al gobierno, los miembros de la trama Ergenekon podrían haber planeado un golpe para 2009 con el fin de arrebatar el poder al gobierno y restituírselo al Estado Profundo.

Desde 2007, la policía ha practicado cientos de detenciones entre altos cargos militares y miembros de los servicios de inteligencia mediante las llamadas «oleadas» Ergenekon. Junto con estos, también han sido detenidas decenas de periodistas y abogados a quienes se acusa de colaborar con Ergenekon por motivos pecuniarios o ideológicos. Los intelectuales liberales, que forman un grupo reducido pero bien organizado, y la clase media, más amplia, han advertido que el gobierno democrático corre el peligro de incurrir en prácticas intimidatorias asociadas por lo común con el Estado Profundo. Las acusaciones contra la trama Ergenekon —signo de los tiempos— dependen en gran medida de pruebas digitales: escuchas telefónicas, mensajería instantánea y archivos informáticos, lo que demuestra las crecientes habilidades cibernéticas de los servicios de inteligencia del país.

Bilal Şen no tuvo relación alguna con todo aquello, pero su diligencia, su compromiso y su vigor juvenil lo acercaban más a la nueva Turquía que a la vieja. Con todo, como la mayoría de la población, era muy consciente de lo delicado que era el contexto político en el que se movía. Lo último que deseaba un policía turco era convertirse en un pobre títere atrapado en la lucha entre el Estado Profundo y el gobierno democráticamente constituido. Casi todos los turcos evitaban en la medida de lo posible discutir en público acerca de Ergenekon, pero todos sabían que la investigación sobre el caso era el telón de fondo de la mayoría de los casos criminales de mayor relevancia, tuvieran o no implicaciones políticas.

Bilal tendría que andarse con cuidado, pero no estaba dispuesto a abandonar la búsqueda.

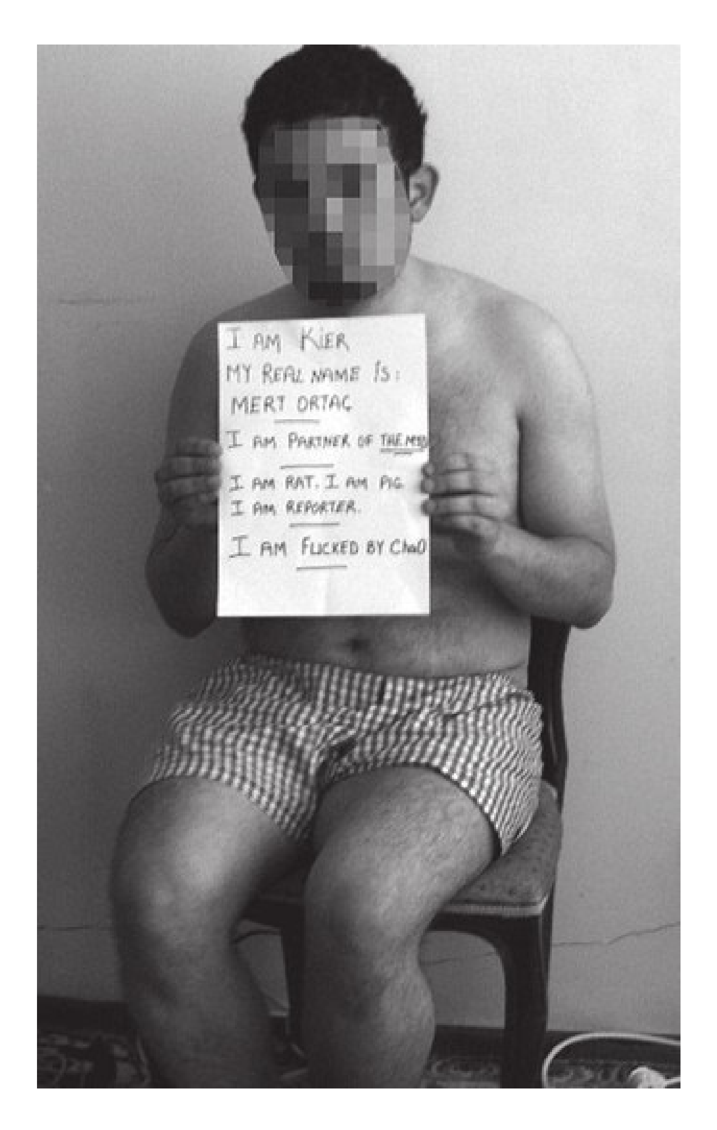
En Pittsburgh, él y Mularski trabaron una sólida amistad y el agente del FBI compartió con él toda la información que pudo sobre Cha0. Entre los dos, empezaron a confeccionar un expediente. Mularski disponía de un amplio archivo reunido durante su etapa como infiltrado en Dark Market, y Şen aportaba su capacidad para descifrar el jeroglífico turco. El inspector quería examinar la personalidad de Cha0 para ver si encajaba con la de algún delincuente informático conocido en su país: numerosos documentos fueron escaneados y circularon entre Ankara, Estambul y Pittsburgh.

Por si las cosas no fueran ya bastante confusas, los acontecimientos tomaron un nuevo derrotero tras el regreso del inspector Şen a Ankara. Una extraña imagen había empezado a circular por la red.

Bilal no podía contener su rabia y su frustración. El agente Mularski le había enviado una fotografía aparecida en la web de Haber 7 y en la revista *Wired*, con sede en San Francisco. En ella se veía a Kier, el hombre misterioso, sentado en ropa interior en una silla sujetando, parece que a la fuerza, un folio en el que se leía:

1. Soy Kier, mi verdadero nombre es Mert Ortaç
2. Soy socio de los medios de comunicación
3. Soy una rata. Soy un cerdo
4. Soy periodista
5. Cha0 me ha jodido

La mitad de la policía de Estambul había buscado a Kier —o Mert Ortaç, por llamarlo por su verdadero nombre— en vano. Pero Cha0 no solo había conseguido dar con él, sino que lo había secuestrado y humillado. Era muy posible que su vida corriera peligro. ¿Qué demonios estaba pasando?



Bilal Şen partía de la base de no creer nunca a pies juntillas nada de lo que se ve en la red. Como visitante asiduo de foros criminales y estudioso del comportamiento de las personas en internet, sabía que la gente miente, engaña, exagera, falsea y conspira sin necesidad de razón alguna. Pero la historia de Dark Market en Europa, y sobre todo en Turquía, iba aún más allá y daba pie a auténticos casos de vileza, espionaje y traición. Y esa historia parecía no tener fin.

PARTE II

28

CHAO, CHA0

Gracias a sus investigaciones con Keith Mularski, el inspector Şen sabía que Cha0 tenía una web propia: Crimeenforcers.com (juego de palabras con la expresión *law enforcers* —«fuerzas de la ley»—, a la que los delincuentes se referían desde hacía tiempo por sus iniciales, LE, dada la frecuencia con que aparecía en los foros de internet).

En la página principal de Crime Enforcers, Cha0 daba a conocer sus fines y servicios:

> Somos una organización privada dedicada al desarrollo. Nuestra especialidad es la ingeniería electrónica e informática. Si necesita *hardware* especial (sobre todo alta tecnología) o *software* cuya producción, e incluso mención, está prohibida en su país por razones legales, etc., ha llegado al sitio adecuado.
>
> Ofrecemos desarrollo anónimo y deslocalizado para sus proyectos. Los fines a los que vaya a dedicar el *hardware* y el *software* que nos solicite no nos interesan.
>
> Huelga decir que para nosotros su privacidad es capital y que no compartiremos sus datos con nadie bajo ningún pretexto. No necesitamos nombres, direcciones, etc., solo su correo electrónico. Se le adjudicará un certificado y una cuenta segura para acceder a nuestro foro privado al objeto de que pueda realizar un seguimiento de su producto. También podrá hacer llegar sus consultas a los ingenieros responsables de su proyecto.
>
> Si ha accedido a esta web, significa que ya nos conoce. Nuestros productos no son baratos y no estamos abiertos a formar sociedad con nadie. Si quiere que sus sueños se hagan realidad, necesitará el dinero indispensable para invertir en ellos. Las consultas acerca de su proyecto también son de pago.

Si uno sabía leer entre líneas, el plan de negocio de Cha0 era evidente. Lo que ofrecía eran servicios logísticos y asistencia a personas interesadas en iniciarse en la delincuencia informática. En lugar de delinquir, prefería ayudar a los usuarios menos experimentados a introducirse en el sector. La delincuencia telemática empezaba a imitar los modelos de negocio del mundo real.

En otras páginas de Crimeenforcers.com podía consultarse una lista con los productos de Cha0. Los productos estrella eran las clonadoras; en poco tiempo, el servicio de venta de clonadoras por correo adquirió un volumen de negocio considerable.

Crime Enforcers también ofrecía lectores portátiles de tarjetas —datáfonos móviles como los que usan la mayoría de los restaurantes—. A principios de 2007, la policía inglesa destapó en varios puntos del país una red de empleados de gasolineras que se habían hecho con un lote de aparatos salidos, al parecer, del taller del *hacker* canadiense Dron o del de Cha0. Cuando los clientes entregaban su tarjeta de crédito, el empleado, antes de introducirla en la máquina de pago auténtica, la deslizaba a través del lector ilegal, situado debajo del mostrador, y copiaba sus datos.

Crime Enforcers ofrecía un buen número de consejos destinados a facilitar la labor de quienes daban sus primeros pasos en el terreno de la delincuencia informática. Para los más novatos, Crime Enforcers disponía de tutoriales en vídeo en los que un avatar de Cha0, dotado de una voz electrónica que conservaba el timbre y la cadencia de su dueño, daba instrucciones y consejos sobre cómo elegir un buen cajero automático antes de perpetrar un delito.

En los vídeos se explicaba, por ejemplo, que no valía la pena instalar clonadoras en cajeros de zonas con un elevado índice de inmigración ilegal (se les daba poco uso, había muchos testigos potenciales y demasiada competencia). Por el contrario, se aconsejaba instalarlas cerca de locales nocturnos, «donde los niños ricos utilizan a menudo las tarjetas de crédito de sus padres».

Cha0 se convirtió en uno de los proveedores de confianza de la industria criminal y su nombre empezó a circular por internet. A partir de ese momento, lo importante era consolidar su reputación y evitar ser localizado.

Uno de sus rasgos característicos era el uso del *globish*, un idioma auxiliar formado a partir de un inglés macarrónico, que se ha convertido en la lengua franca de la red y que hace las veces de cifra capaz de comunicar a brasileños con coreanos y a búlgaros con indonesios; en poco tiempo, incluso la ortografía y el uso de los anglófonos nativos comenzó a adquirir rasgos

peculiares en internet. Así pues, uno podía suponer cuál era el origen de tal o cual mensaje en un foro, pero por lo general resultaba imposible identificar con certeza la nacionalidad de su autor o autora.

No ocurría lo mismo con el ruso o el chino. Los mensajes de las webs criminales rusas estaban plagados de jerga local; un lingüista habría podido descifrarla, pero solo un superdotado habría sido capaz de imitarla sin ponerse en evidencia como extranjero. Los agentes del FBI podían moverse a su antojo por los foros de lengua inglesa, pero en las webs rusas difícilmente habrían podido pasar de la página de registro. Y es que, aunque en ocasiones los cuerpos de seguridad e inteligencia estadounidenses han echado mano de hablantes nativos de ruso y chino, nunca han disfrutado de los recursos económicos y lingüísticos necesarios para hacerse con el control de una página rusa, cosa que sí lograron en parte con Dark Market.

En las páginas en inglés, la identidad de los interlocutores nunca deja de ser una incógnita. La red como medio permite, e incluso fomenta, que sus usuarios cambien de personalidad. Esto no es prerrogativa del mundo del hampa. Las webs de citas han sido desde siempre uno de los lugares con mayor concentración de mentirosos. En las salas de chat, los usuarios proyectan un talento y una importancia que rara vez se corresponden con la realidad cotidiana de sus vidas. La web alienta estos comportamientos porque los usuarios no tienen la posibilidad de contrastar los rasgos de conducta de sus interlocutores virtuales. La gente sabe que en la red se puede mentir sin miedo a ser descubierto o censurado.

Los delincuentes no solo actúan siguiendo los mismos patrones de engaño, sino que son profesionales de la simulación. Dark Market es buena prueba de ello. El diabólico Devilman, por ejemplo, se presentaba en los chats como un joven vividor aficionado a las mujeres (aunque a la hora de la verdad prefería los *dumps* a buen precio). Sin embargo, cuando los detectives llamaron a la puerta del número 62 de Lime Tree Grove, en Doncaster, una casa pareada de dos plantas donde residía John McHugh, el *alter ego* de Devilman, les abrió la puerta un hombre de sesenta y pocos años cuyas primeras palabras al ser arrestado fueron: «¿Les importa si antes me pongo la dentadura?». Ante el tribunal, en el momento de la sentencia, alegó como atenuante haber sufrido un trasplante de cadera y encontrarse a la espera de una segunda operación, cosa que restringía seriamente su movilidad.

Pero los delincuentes informáticos profesionales deben generar confianza para hacer negocio: la reputación es crucial. En Dark Market solo era posible adquirir el título de vendedor demostrando a administradores y clientes que

uno era capaz de sacar al mercado tarjetas de crédito robadas que funcionasen de verdad. Las transacciones estaban supervisadas por cinco administradores (tres después de la expulsión de JiLsi y la detención de Matrix): Master Splyntr, Shtirlitz y Cha0 (más tarde se les sumaría Lord Cyric).

Cha0 ingresó en Dark Market en febrero de 2006, pero sus considerables habilidades le permitieron escalar rápidamente en la jerarquía. En cuanto hubo consolidado su posición como príncipe de Dark Market, pudo centrarse en su verdadera estrategia de negocio. Lo que él quería era convertirse en el primer vendedor de clonadoras y lectores ilegales del mundo. Esos aparatos tenían mucha demanda y, si conseguía crear un monopolio, podría pasar a la fase siguiente de su plan de maximización de ingresos con un esfuerzo mínimo.

El de Estambul también tenía a su cargo el vital servicio de fideicomiso de Dark Market, acaso el eje en torno al cual giraba toda la página. Como mediador de confianza, aseguraba que los compradores y los vendedores de tarjetas y otros datos ilegales no se estafasen mutuamente. En ese sentido, Dark Market actuaba como una organización mafiosa en sentido estricto. La web ejercía como policía o árbitro del mercado criminal, de la misma manera que los «hombres de honor» empezaron su andadura ofreciendo protección a los mercados agrícolas de Sicilia en la segunda mitad del siglo XIX, antes de pasarse al tráfico de armas y los permisos de obras.

La reputación de Cha0 como gestor fiduciario se benefició de su éxito como vendedor al por mayor de máquinas clonadoras. Todo el mundo confiaba en Cha0. Él, en cambio, no se fiaba de nadie. Jamás reveló su dirección IP; jamás envió ningún mensaje sin encriptar que pudiera implicarlo en una fechoría, y nadie pudo dar nunca con su localización digital.

Una vez que Bilal Şen aceptó que Cha0 había creado en el ciberespacio un agujero negro donde se mantenía a salvo y fuera de la vista de la policía, decidió optar por métodos policiales más tradicionales para seguirle la pista a su sospechoso. Y es que la paciencia ha sido siempre un factor de suma importancia en la labor de los ciberpolicías.

29

GUERRAS CLON

Estambul, Turquía, 2008

Aunque angustiado por el hecho de que Cha0 pudiera gozar de la protección de las altas esferas, Bilal Şen perseveró en su búsqueda. Le prometió al agente Mularski que seguirían en estrecho contacto tras su regreso a Estambul. Habían discutido la posibilidad de solicitar los servicios de fideicomiso de Cha0 a través de Dark Market, por si de esa manera podían hacerlo salir de su guarida, pero pronto se dieron cuenta de que la operación era demasiado laboriosa y su éxito, poco probable.

El otro dato que conocían, por supuesto, era que Cha0 comerciaba con clonadoras. Estaba visto que en la red era imposible dar con él. Pero si Cha0 vendía aquellas máquinas, pensaba Bilal, sus operaciones tenían dos puntos débiles: la fabricación y el envío.

La instalación de clonadoras en cajeros automáticos estaba convirtiéndose en algo tan habitual en Turquía que cada vez eran más los agentes de policía formados para detectarlas. Muchos de los dispositivos eran de factura tosca, y sus usuarios, simples aficionados. Sin embargo, al leer los informes de detención y confiscación, el inspector observó que en determinadas zonas no solo mejoraba su diseño, sino que parecían fabricarse en cantidades cada vez mayores. En alguna parte tenía que haber un taller. Los servicios de inteligencia alertaron a Şen de la posible presencia de fábricas de clonadoras en Rumanía y Bulgaria, así que solicitó ayuda a las fuerzas de policía de esos países. La otra posibilidad era que Cha0 disfrazara sus operaciones como negocios legales y comprara sus aparatos a fabricantes de lectores de tarjetas con licencia en territorio turco.

Una vez adquiridas las clonadoras, Cha0 debía distribuirlas. Mularski y Şen habían hallado pruebas que sugerían que sus productos viajaban a lugares tan lejanos como Estados Unidos, Nueva Zelanda y Sudamérica, en ocasiones en cantidades considerables. De ser así, era poco probable que se sirviera de mensajeros personales. A la vista de las cifras que se barajaban, era

imposible. Bilal se preguntó cuáles podían ser los motivos de aquel aumento en la productividad, pero no llegó a ninguna conclusión.

Lo que Bilal no sabía era que un año antes, a finales de la primavera de 2007, Cha0 había tenido un enfrentamiento con Dron, el canadiense especializado en clonadoras al que el Servicio Secreto y el detective Spencer Frizzell estaban a punto de detener. Según Cha0, Dron era «un tipo difícil» que acababa con los nervios de sus clientes y que, por lo tanto, socavaba la reputación de Dark Market. La gran cantidad de mensajes a favor de Dron sugería que los motivos de Cha0 podían ser otros. De hecho, algunos miembros del foro sostenían que Cha0 atacaba a Dron por motivos personales.

Alrededor de un mes antes de que el joven canadiense especializado en la venta de clonadoras cayera en manos del detective Frizzell, Cha0, valiéndose de su cargo de administrador, anunció que Dron sería expulsado de Dark Market sin posibilidad de readmisión. Cha0 ya podía poner en marcha su plan para dominar el mercado y pasar a la acción.

Dark Market representaba una plataforma vital para los negocios de Dron: buena parte de sus máquinas se vendían gracias a los anuncios de pago que colgaba en el foro. Dark Market era también el principal vehículo publicitario de Crimeenforcers.com, a través de la cual Cha0 vendía sus propias clonadoras. Cha0, además, ofrecía a los futuros tarjeteros paquetes de soluciones en los que se incluían formación, manuales y todo el equipo necesario para introducirse en el negocio.

Sin embargo, cuando Dron desapareció de la circulación, el modelo de negocio cambió: las partes interesadas dejaron de poder comprar sus clonadoras; a partir de entonces tendrían que alquilarlas. Cha0 seguiría enviándoselas, pero con una leve modificación.

Tras la expulsión de Dron, Cha0 aumentó el precio de las máquinas: alquilarlas costaría en adelante siete mil dólares, frente a los cinco mil que hasta entonces costaba su compra. Tras el pago, además de la clonadora, a los clientes se les enviaba un teclado. Lo que debían hacer era instalar la clonadora en la ranura del cajero automático y el teclado encima del de la máquina. Así, cuando los clientes insertasen su tarjeta y tecleasen el número secreto, todos los datos quedarían registrados en el teclado falso y en la clonadora. Posteriormente, los dispositivos eran retirados y el cliente de Cha0 podía volcar la información en un ordenador con un cable USB.

Con las clonadoras de Dron, el cliente podía utilizar la información para obtener fondos de manera fraudulenta, pero con las de Cha0 los datos

descargados en el ordenador permanecían encriptados. Y la única persona que disponía de la clave para descifrar la información era… Cha0. De modo que el joven delincuente que con tantas precauciones había instalado la clonadora y el teclado en el cajero automático no podía ponerse a clonar tarjetas por sí solo; antes debía enviar la información a Estambul. Desde ahí, Cha0 organizaba la retirada del dinero. En cuanto el dinero llegaba a sus manos, mandaba una parte al cliente que había hecho el trabajo sucio. Así funcionaba el sistema de alquiler de clonadoras; como estrategia, era mucho más lucrativa que las ventas de Dron.

Como modelo de negocio, era francamente atrevido. Si lograba tener éxito, Cha0 podría amasar sumas inconcebibles a base de adjudicarse un amplio porcentaje de las operaciones de clonación de tarjetas del mundo entero. Lo único que tenía que hacer era continuar con la producción y el envío de clonadoras. En principio era fácil. Aunque, por supuesto, podía llegar un día en que la competencia tratara de debilitar su estrategia e incluso reinstaurar el viejo modelo de la venta directa. Pero, hasta entonces, y gracias a que controlaba el foro más influyente del mundo anglófono, Cha0 podía seguir viviendo a cuerpo de rey.

En 2008, Estambul llevaba camino de convertirse en la ciudad con mayor crecimiento del mundo. Hacía quince años que la población no dejaba de aumentar de forma poco menos que descontrolada y la ciudad albergaba por entonces a unos quince millones de personas, de las cuales se estimaba que dos millones eran inmigrantes no registrados, no solo extranjeros, sino también turcos y kurdos de Anatolia que emigraban a la ciudad del Bósforo, el imponente paso de agua que separa Europa y Asia.

A diferencia de muchas ciudades de Asia oriental, principalmente de China, Estambul no ha conseguido este formidable y enérgico crecimiento a expensas de su rutilante pasado. La historia se palpa en casi todos sus edificios. Cada rincón transmite el eco de las ricas tradiciones de más de un milenio de historia bizantina y seiscientos años de poderío otomano, dos de los imperios más mágicos, violentos, célebres y abrumadores de todos los tiempos. Contrariamente a la imagen que de él se ha divulgado, el Imperio otomano fue conocido durante buena parte de su historia por la tolerancia que sus gobernantes mostraban hacia los tres «pueblos del Libro»: judíos, cristianos y musulmanes. Su reputación violenta tiene su origen en las sangrientas masacres del pasado más remoto, y solo resurge durante la lenta agonía de los siglos XIX y XX.

Ya en tiempos de la República turca, nacida de las cenizas del imperio tras la primera guerra mundial, Estambul ha atravesado momentos difíciles: el primero, con el traspaso de la capitalidad del país a Ankara, una advenediza anatolia situada al este; y de nuevo, durante la guerra fría, cuando un ejército despiadado intentó acabar con el espíritu independiente de la ciudad. Las infraestructuras empezaron a tambalearse y la gente comenzó a emigrar, con lo que el número de habitantes se redujo a dos millones. Sin embargo, a partir de principios de la década de 1990, Estambul ha dado grandes pasos para recuperar su lugar entre las ciudades más dinámicas y fascinantes del mundo.

Abarrotada, bulliciosa y exuberante, con una actividad económica que va y viene entre los sectores europeo y asiático, Estambul, con sus decenas de miles de coches y camiones destartalados abarrotando los dos puentes intercontinentales, a veces puede resultar sofocante. En el lado europeo, el tráfico avanza a paso de caracol en los alrededores de la plaza Taksim o a lo largo de Dolmabahçe, los antiguos jardines imperiales, orientados en dirección a Asia. Incluso cuando el tiempo es fresco, el polvo reseca la garganta. Pero en la última década, la ciudad ha sido un hervidero de oportunidades —artísticas, comerciales y políticas—; además, hay pocos placeres mayores que tomar un transbordador en la parte europea y dirigirse, mientras se contempla el Bósforo, a la parte asiática para echarse una deliciosa cena entre pecho y espalda en Kadıköy.

Desde la llegada al poder del AKP, y pese al miedo de que pueda ser una quinta columna del fundamentalismo islámico, la joven clase media de Estambul ha querido aprovechar el momento económico y ha abrazado la industria, el diseño, la alta tecnología y los servicios, creando empresas capaces de competir con las mejores de Europa, América y Asia.

Naturalmente, patrullar la ciudad es una auténtica pesadilla, sobre todo porque los habitantes se fían poco de un cuerpo que durante décadas simbolizó más que ningún otro la represión de los aparatos del Estado.

Con los nuevos delitos, nacen nuevas razas de policías, y como Bilal no guardaba relación alguna con las viejas tradiciones del Estado Profundo ni se había enemistado con personajes especialmente poderosos, fue bien recibido en Estambul cuando llegó desde Ankara, la capital, decidido a desmantelar la red de distribución de Cha0.

Puesto que se trataba de Estambul, era como buscar una aguja en un pajar. Los negocios de exportación e importación legales, semilegales e ilegales son desde hace siglos la base económica de la ciudad, puerta de entrada y de salida de toda clase de mercancías. Desde la década de 1960, los

electrodomésticos llegan en grandes cantidades a Estambul a través de los Balcanes procedentes de Alemania, adonde unos dos millones de turcos emigraron en los años sesenta como *Gastarbeiter*, o trabajadores invitados. El volumen del negocio se disparó con la caída de la Unión Soviética y la apertura de nuevos mercados en Rusia, Ucrania, el Cáucaso y varias repúblicas centroasiáticas de lengua túrquica.

Pero por algún sitio había que empezar, así que Bilal seleccionó las tres mayores compañías de mensajería de la ciudad. Él y sus ayudantes dedicaron medio día a instruir a los empleados de las empresas en el arte de distinguir máquinas clonadoras. Suelen registrarse como piezas sueltas de vehículos o herramientas para maquinaria. Incluso facilitaron clonadoras al personal para que se familiarizaran con su forma y peso.

Los días transcurrían sin novedad, y el inspector Şen decidió regresar a la central de Ankara. Pasaron las semanas y empezó a sentir un desaliento que a esas alturas ya le resultaba conocido. Justo un mes después, llegaron buenas noticias desde Estambul: un hombre se había presentado en una de las empresas de mensajería con un paquete con destino a Finlandia. Había resultado ser una clonadora. La recepcionista llamaba desde la trastienda con la noticia de que el paquete incluía también un teclado.

«¡Bingo!», pensó Bilal mientras le decía a la recepcionista que dejara marcharse al remitente: las cámaras de vigilancia ya habrían captado su imagen. Después de muchos meses, por fin el inspector había dado con una pista. Como era de suponer, el hombre había utilizado un documento de identificación falso, pero entonces apareció la segunda pista. El sospechoso había dejado tres números de teléfono, y uno de ellos era real. Realizaron una consulta para identificar al titular legal del teléfono móvil, pero no parecía encajar con ningún delincuente. Con todo, decidieron hacer un seguimiento del número y descubrieron que el hombre del paquete lo utilizaba. Era un número activo.

«Este tipo podría conducirnos hasta Cha0», pensó Bilal.

Pero el inspector se enfrentaba a un dilema. Fue entonces cuando la agencia de noticias Haber 7 publicó la fotografía de Mert Ortaç, el *hacker* humillado, y la presión se dejó sentir aún con mayor fuerza sobre la policía de Estambul, que tenía el deber de encontrar a Ortaç, y sobre Bilal, cuyo objetivo principal era Cha0. Había que agilizar el proceso. Pero, al mismo tiempo, sabía que no podía permitir que la impaciencia pusiera en peligro la operación.

Con el secuestro de Ortaç, Cha0 había dado por primera vez señales de miedo y vulnerabilidad. Lo que nadie sabía era por qué lo habían trastornado tanto las declaraciones de Ortaç a Haber 7.

Cha0 sabía que Ortaç era turco y creía que podía trabajar como confidente de la policía. Además, imaginaba que Ortaç era un fugitivo y que estaba asustado. Si la policía lo encontraba antes que Cha0, existía el peligro de que descubriera todo el tinglado.

Pero ¿quién era Mert Ortaç y cómo había llegado a involucrarse en aquel delicado asunto? Todo había comenzado durante la primavera anterior, cuando, sin saberlo Ortaç, Matrix y JiLsi estaban a punto de ser detenidos, lo que pondría fin a la fase uno de la operación Dark Market y daría pie a la fase dos.

PARTE III

En el curso de un año, Dark Market me había obligado a recorrer un largo camino: desde la sede de Google hasta un restaurante de Cihangir, el barrio chic de la Estambul europea, justo debajo de la plaza Taksim. Ante mí danzaba la sonrisa eufórica de Mert Ortaç. Tras pasar varias horas en su compañía, concluí que el adjetivo *malicioso* encaja con Mert mejor que con nadie más en el mundo.

Durante una abundante cena en Kadıköy, mi amigo Şebnem y yo dejamos nuestros iPhones encima de la mesa. De pronto, ambos recibimos a la vez sendos mensajes. El mío había sido enviado desde el teléfono de Şebnem, y el de Şebnem, desde el mío. En ambos ponía: «¡Saludos de Mert!». Mientras leíamos los mensajes, Mert dejó escapar una risotada estentórea desde el otro lado de la mesa y dijo que había conseguido piratear el servicio de *roaming*. Por lo tanto, continuó, podía enviar mensajes desde y a cualquier teléfono del mundo. En las manos equivocadas (por ejemplo las de Mert), trucos como ese podían provocar una serie inacabable de tragicómicos enredos shakesperianos.

Había empezado a escribirme con Mert durante su estancia en prisión, desde donde me había referido fragmentos de una historia cuya audacia dejaba a la altura del betún a las demás leyendas sobre Dark Market. En la mayoría de mis intercambios con personas relacionadas con Dark Market, había notado que me escondían información; Mert, en cambio, me abrumaba con datos, anécdotas y lances de lo más alucinantes.

Resulta indispensable que *hackers*, delincuentes informáticos y ciberpolicías mantengan un control absoluto sobre sus distintas parcelas vitales: deben tener muy claros los límites entre los terrenos de lo real y de lo virtual, a fin de no actuar en uno como si se encontraran en el otro. Pero desde hacía tiempo Mert era incapaz de distinguir la verdad de la ficción.

Si Mert hubiese sido tan solo un mistificador absurdo y sin remedio, todo habría resultado muchísimo más fácil. Seguirles la pista a los *hackers* y policías vinculados con el caso Dark Market ha sido una de las experiencias más enervantes en toda mi andadura periodística. Sin embargo, mi exasperación ha rebasado todos los límites al analizar qué parte de lo que decía Mert era cierto. Acaso sería mejor decir que gran parte de lo que decía era verdad y, en general, verificable, solo que adornado con tanto aliño y floritura que, en ocasiones, parecía querer decir otra cosa. Curiosamente, cuando Mert mentía de forma flagrante, lo hacía a menudo con respecto a detalles banales y de fácil comprobación. Me dijo, por ejemplo, que había

nacido el 10 de abril de 1982, cuando en realidad había nacido ese mismo día pero cuatro años más tarde.

En los capítulos que siguen, refiero la historia de Mert tal como él me la contó. Existen, sin embargo, dos puntos importantes en que sus explicaciones no encajan, o por lo menos yo no he podido confirmarlas; es más, uno de los testimonios refuta de plano la versión de los hechos de Mert. En su momento, el lector será debidamente avisado.

La prueba definitiva de la credibilidad de Mert se refleja en su respuesta a la pregunta que ha traído de cabeza a muchos estudiosos del submundo virtual desde los inicios de Dark Market: ¿quién era Lord Cyric?

30

EL MUNDO ONÍRICO DE MERT ORTAÇ

Estambul, Turquía, mayo de 2007

Mert Ortaç respiró hondo al entrar en el salón de la opulenta mansión. El techo le recordaba al de la *suite* Sultán del Çirağan Palace, una obra maestra edificada a finales del siglo XIX a instancias de su alteza imperial, el sultán Abdülaziz, y recientemente adquirida por la cadena hotelera Kempiński. Volutas de pan de oro adornaban sillas y sofás, y los arabescos del papel de la pared refulgían a la luz del sol.

De hecho, el Çirağan Palace quedaba a ochocientos metros de la mansión, encerrada en un complejo férreamente vigilado. Los agentes patrullaban los alrededores y lanzaban hoscas miradas a todo el que intentara aparcar cerca. Sito en un extremo del barrio de Beşiktaş, el palacete miraba majestuoso desde lo alto de su colina del lado europeo hacia el estrecho del Bósforo y la parte asiática. Lo más llamativo era que en el salón al que habían conducido a Mert no colgaba ningún retrato de Kemal Atatürk, el venerado fundador de la Turquía moderna. Los retratos de Kemal son de rigor en todo el país, y no solo en los despachos públicos y privados: a menudo puede encontrárselos en todas las habitaciones de un edificio. Mas no en esa, pese a formar parte de las dependencias regionales del Milli İstihbarat Teşkilati (MİT), la Agencia Nacional de Inteligencia de Turquía.

Por lo común, Mert reaccionaba ante las situaciones comprometidas esbozando una contagiosa sonrisa maliciosa o huyendo sin más. Dadas las circunstancias, ninguna de las dos opciones parecía apropiada. Mert se quedó mirando a los elegantes camareros que servían té y café. Lo que más le llamaba la atención eran los blancos guantes inmaculados con que ponían las cosas sobre la mesa frente a él. Notaba una sensación irreal de bienestar y emoción controlada. Pero no duró mucho.

Con él estaba un compañero del Instituto Tecnológico de Ciencias Avanzadas, pero no conocía a las otras tres personas que lo habían saludado. En cuanto los camareros se hubieron retirado en silencio, los tres hombres

dirigieron su atención hacia Mert. «Deseamos hacerle unas cuantas preguntas», dijo uno. Luego colocaron sobre la mesa una grabadora digital.

Al poco rato estaba sudando debido a la presión del interrogatorio. Sin embargo, el propósito de la entrevista no era someterlo a un tercer grado. Durante seis horas y media, Mert tuvo que resolver un sinfín de enrevesados problemas matemáticos. En circunstancias normales, ni se le habría pasado por la cabeza hacerlo sin la ayuda de un ordenador. Sus anfitriones le habían pedido que se sirviese de una metodología corriente en el campo del cifrado consistente en dividir el número cincuenta y dos en números impares. Eran problemas de matemática avanzada y para resolverlos no contaba con más ayuda que un lápiz y un folio de papel.

El joven programador no había conseguido superar el examen de selección para entrar en la lista de candidatos a un contrato de pruebas en el cuerpo de inteligencia. Había superado las pruebas de lengua extranjera (inglés) y de matemáticas, pero había suspendido clamorosamente la de lengua turca. Pese a todo, los examinadores habían quedado fascinados con sus habilidades informáticas. Su pericia como programador era sobresaliente y contaba con un historial admirable, de modo que lo admitieron como colaborador externo.

En 2003, Mert se hallaba bajo investigación por fraude. No tenía más que diecisiete años, pero se las había arreglado para romper el código de las tarjetas inteligentes de la plataforma de televisión por satélite turca Digiturk. Esa podía ser una lucrativa fuente de ingresos. Digiturk había conseguido poco antes los derechos para retransmitir la Süper Lig, la popular primera división de fútbol del país. Para decodificar el canal y poder disfrutar de los partidos, los abonados debían adquirir una tarjeta inteligente e insertarla en el receptor de la señal del satélite.

Cuando Mert descubrió cómo piratearlas, empezó a reproducirlas para venderlas de forma ilegal en las calles de Estambul, lo que le permitió amasar una suma estimable. Todo el dinero que ganaba lo gastaba al momento en fiestas para sus amigos de Ankara, a quienes invitaba a Estambul corriendo con todos los gastos de viaje y alojamiento. Jamás supo administrar el dinero, ni siquiera después, cuando empezó a ganar cantidades considerables como tarjetero.

Mert daba tanta importancia a los amigos porque necesitaba afecto. Tuviera o no consciencia de ello, Mert utilizaba el dinero de Digiturk para comprar amigos, y Estambul estaba lleno de veinteañeros encantados de

confraternizar con cualquiera dispuesto a financiar sus costosas fiestas. Claro que, cuando se acababa el dinero, los compañeros desaparecían.

Por otra parte, Mert no veía la hora de demostrar que era alguien especial (y a la vista de su talento informático, sin duda lo era), por lo que a menudo exageraba sus logros. A medida que fue acentuándose esa tendencia, la conciencia de Mert empezó a fluctuar entre la realidad y la fantasía. Según parece, muy pronto perdió la capacidad de distinguir entre ambas. Su confusión era tal que, de haberse sometido a un detector de mentiras, la máquina tanto podría haber rebasado el nivel máximo como no haber registrado la menor alteración. Por lo demás, eso significa que su adaptación a la cultura de internet —el valle de las mentiras— fue sencilla.

Tras pasar por varios trabajos en empresas relacionadas con las tecnologías de la información, en junio de 2006 Mert fue contratado por la concesionaria local de Toshiba, cuyo departamento de personal ignoraba que se hallaba bajo investigación por el fraude de Digiturk. El comportamiento de Mert no tardó en extrañar a sus compañeros de trabajo, a quienes les pareció cuando menos sospechoso que tuviera un certificado de licenciatura en ciencias de la criptología por la Universidad de Cambridge.

La junta de la universidad, según rezaba el certificado, «expide el presente diploma como prueba en la ciudad de Londres en Cambridge, a día 22 de junio de 2004».

Dicho así, parecía significar que le habían hecho entrega del diploma en el Cambridge Arms de Londres. Dondequiera que hubiera tenido lugar aquella ceremonia ficticia, el certificado era tan burdo que apenas cabía llamarlo «falsificación».

Uno de sus compañeros en el departamento de tecnologías de la información de Toshiba estaba desconcertado por la frecuencia con que Mert se vanagloriaba de su vinculación con el cuerpo nacional de inteligencia. Su compañero también había colaborado con la policía secreta, sobre todo a finales de la década de 1990, cuando la agencia todavía no disponía de una división especializada en informática, y por eso mismo sabía que esas cosas no se dicen en público. Los continuos comentarios de Mert sobre su estrecha relación con la inteligencia del país fueron lo que despertó más recelo. Toshiba, no obstante, lo mantuvo durante seis meses porque, siempre que sus jefes le pedían que resolviera un problema, daba con la solución. Sabían que era inteligente, pero algo les decía que valía más no perderlo de vista.

Una tarde Mert recibió una llamada de su enlace con el cuerpo de inteligencia. Había que realizar un peritaje forense de varios discos duros y

ordenadores salidos, según parece, de la nada. Su misión consistía en recuperar archivos, romper todas las contraseñas posibles y reunir el material incriminatorio. La entidad tenía como cometido principal garantizar la seguridad de Turquía, y para ello había que realizar un seguimiento de multitud de organizaciones que el gobierno consideraba vinculadas al terrorismo.

Hacia finales de 2006, Toshiba despidió a Mert. Su actitud era inadecuada y se jactaba en exceso de sus dudosas hazañas con las tarjetas de crédito, lo cual no le impedía solicitar una y otra vez préstamos y pluses a sus colegas.

Mert, sin embargo, sostuvo que había sido él quien abandonó Toshiba por instrucción de sus superiores en el servicio de inteligencia. Según él, la intención era encontrarle trabajo como infiltrado.

Poco antes de incorporarse al nuevo puesto, su enlace lo puso a trabajar en un disco duro que formaba parte de una investigación sumamente delicada. En control querían saberlo todo sobre todos y cada uno de los archivos del disco, los visibles y los ocultos, los legibles y los encriptados. El disco pertenecía a un miembro veterano de una organización de izquierdas clandestina conocida por las siglas DHKP/C.

Durante la década de 1990 y principios de la siguiente, el DHKP/C había sido una de las organizaciones de izquierdas más violentas y efectivas vinculadas a la lucha armada en Turquía. El Partido-Frente Revolucionario para la Liberación del Pueblo (el Partido era el brazo político y el Frente, en teoría, el militar) era un grupo escindido del Dev Yol, un movimiento revolucionario más amplio que se llevó la peor parte durante la represión militar de las décadas de 1970 y 1980.

No eran aficionados; se tomaban la actividad política y terrorista con la máxima seriedad y se dedicaban sobre todo a atacar la colaboración entre el imperialismo —así lo calificaban— de la OTAN y el estamento militar turco. La organización consiguió atentar con éxito contra ciudadanos turcos, estadounidenses y británicos relacionados con el mundo de los negocios o con el ejército. A diferencia de la mayoría de los grupos armados de izquierdas, el DHKP/C presumía de poseer un sofisticado dispositivo de contrainteligencia, lo que lo convertía en uno de los principales objetivos de la Agencia Nacional de Inteligencia.

Los agentes se habían incautado de un ordenador portátil, que entregaron a Mert en la mansión donde lo habían entrevistado la primera vez y donde siempre trabajaba. El agente que se lo entregó le informó de que el usuario era miembro de una web llamada Dark Market. Como también él era experto en

informática, le dijo a Mert que había seguido las conexiones de Dark Market hasta Singapur, donde le había perdido la pista, pero que sospechaba que podía tratarse de un *proxy*. Ignoraba quién podía estar detrás de la web, aunque las pruebas sugerían que el DHKP/C podría haber recurrido al tarjeteo como medio para maximizar sus ingresos. Era posible que el grupo estuviese investigando si los *botnets* podían serles útiles para alcanzar sus objetivos.

Dark Market ya no era tan solo una web de delincuentes, sino un medio de financiación de una organización terrorista.

El agente le preguntó a Mert si sabía algo acerca de esa página.

Mert dijo que no. Siguió el rastro de la web hasta Singapur, pero no halló el modo de ir más allá. De hecho, eso se debía a los denodados esfuerzos de Grendel. No obstante, Mert le dijo al agente que conocía a alguien que podía estar familiarizado con Dark Market.

Mert estaba agotado. El centro de inteligencia esperaba siempre que terminara los encargos de un día para otro. Por entonces, Mert había empezado a trabajar en la filial turca de la Fox. News International, la empresa de Rupert Murdoch, no era la propietaria exclusiva de Fox Turquía, ya que, según la ley turca, al menos el cincuenta y uno por ciento de las acciones debían estar en manos de un ciudadano del país. El accionista mayoritario de la cadena era un exdiplomático conocido por sus vínculos con la policía y los servicios secretos. Sus colegas en la Fox notaban que Mert a menudo, si no siempre, estaba distraído y que le costaba terminar los encargos, no porque no fuera capaz de realizarlos, sino porque siempre estaba haciendo otras cosas.

Uno de los contactos de Mert le había advertido que vigilara a un tal Sadun Özkaya, un adolescente de clase media cuyos padres temían que estuviera yendo por el mal camino. Acababa de salir de prisión y se hallaba bajo investigación por fraude. El contacto de Mert le había encomendado que lo ayudara a enmendarse, lo cual era como pedirle a un lobo que convenza a otro lobo de los beneficios de ser vegano mientras ambos lamen los huesos de un sabroso cordero.

Mert sabía de criptografía y programación, y Sadun era un experto en tarjetas de crédito. Enseguida pusieron sus habilidades en común. Para sorpresa de Mert, Sadun le dijo que era miembro de Dark Market, a la que accedía utilizando dos alias: Cryptos y PilotM. A las pocas horas, Mert Ortaç entraba en la página usando el segundo.

«¡Oh, prodigio! —Debió de pensar Mert mientras exploraba los entresijos de Dark Market—. ¡Qué formidables criaturas son estas! ¡Bella humanidad!

¡Oh, espléndido mundo nuevo que tales gente produce!».

Mert no daba crédito. Inspeccionó hasta el último rincón de la web, leyó los foros, aprendió a imitar el argot de los usuarios e intentó descubrir sus secretos por medios algo menos honestos. Hasta entonces, las aspiraciones delictivas de Mert se habían limitado al terreno de la decodificación y la venta de tarjetas inteligentes. En Dark Market, aprendió los trucos del fraude con tarjetas de crédito. La combinación de ambas habilidades los llevaría, a él y a Sadun, a un terreno algo más pantanoso, aunque económicamente rentable.

Antes, sin embargo, se dedicó a trazar un esquema de Dark Market, cual si de un subterráneo laberinto plagado de trampas y tesoros se tratase. Sus superiores en la Agencia Nacional de Inteligencia querían que hallara pistas sobre el DHKP/C, pero a Mert la información que le interesaba era otra.

Enseguida vio que Cha0, Master Splyntr, Shtirlitz y Lord Cyric eran los miembros clave de la web. Para entonces, JiLsi y Matrix001 ya habían caído.

Le bastaron unos segundos para darse cuenta de que Cha0 era turco, aunque el descubrimiento fue accidental y no tuvo nada que ver con su pericia como *hacker*. Mientras leía los anuncios de clonadoras de Cha0, encontró una imagen al fondo de la cual podía verse el letrero de un establecimiento de kebabs escrito en turco. En otra fotografía, aparecía una clonadora junto a un paquete de detergente turco.

Cuando informó de la fuerte presencia turca en la web, el interés por Dark Market de su supervisor en el cuerpo de inteligencia aumentó: no solo actuaban terroristas de izquierdas en la web, sino que estaba dirigida desde Turquía. Podía tratarse de una pista importante; era preciso seguir investigando. Mert recibió autorización para ponerse en contacto con Cha0 y otros connacionales que frecuentaran los foros de Dark Market. Poco después creyó haber identificado a otro: Lord Cyric.

Mert se puso a buscar en los registros de principios de los años noventa, época en que se popularizó el uso de los BBS o sistemas de tablones de anuncios, una suerte de eslabón entre la mensajería electrónica e internet. Rebuscando entre los mensajes, descubrió algo que lo dejó boquiabierto: los nombres de Cha0 y Lord Cyric aparecían juntos. Concluyó que los dos cerebros de Dark Market se conocían desde hacía mucho tiempo.

31

SERVIDOR DE DOS AMOS

El ficticio Lord Cyric había adquirido popularidad entre los aficionados a los juegos y la informática de los años ochenta y principios de los noventa. Era un dios autoproclamado que rondaba los Reinos Olvidados, un mundo de fantasía dejado de la mano de Dios en que los guerreros erraban en busca de tesoros y oscuros secretos enfrentándose a criaturas con poderes mágicos y ansias de destrucción. Los Reinos Olvidados eran el territorio por el que se movían los aventureros aficionados al juego de rol *Dragones y mazmorras*. Posteriormente, aquel inhóspito país de inspiración subtolkeniana aparecería en multitud de videojuegos, entre ellos, el popular *Baldur's Gate*.

El país fue descrito también en varias novelas basadas a partes iguales en *Dragones y mazmorras* y *El señor de los anillos*. La figura de Lord Cyric desempeñaría un papel clave en la mitología de los Reinos Olvidados, donde encarnaba a un dios de maldad insondable. Ya en relación con el mundo del tarjeteo y Dark Market, Cyric era conocido, entre otras cosas, como el «príncipe de la mentira», y entre sus diabólicos poderes se contaban el engaño y la ilusión, así como el don de promover conflictos e intrigas.

Quienquiera que se ocultara tras ese avatar en Carders Market, Dark Market y otras páginas, lo que deseaba era proyectar el concepto que los jugadores de *Dragones y mazmorras* definían como «maldad caótica», o, lo que es lo mismo, dar vida a un personaje que siembra la confusión y la desesperanza de forma arbitraria allá por donde pasa. La definición encajaba con la afición del Lord Cyric de Dark Market al engaño, la ilusión, el conflicto y la intriga. Pocos tarjeteros llegaron a generar tanta hostilidad como él en el seno de la comunidad. Su especialidad era propagar acusaciones mediante rumores e infundios.

Por razones nunca esclarecidas, Cyric se fijaba un objetivo, por ejemplo RedBrigade, quien tanto se había lucrado gracias a Shadow Crew en Nueva York. A continuación, lo atacaba por todos los flancos para dinamitar su reputación entre los tarjeteros. Indirectas e insinuaciones sobre la identidad de RedBrigade, comentarios en clave sugiriendo que en realidad trabajaba para

las fuerzas de la ley. Su lenguaje era brusco e infantil, aunque a la vez cuidadosamente elaborado con el fin de crear el mayor perjuicio posible al objeto de sus ataques.

Cyric también tenía sus defensores, y ninguno tan incondicional como Cha0. Dotado de un cerebro privilegiado y de un complejo de superioridad a juego, Cha0 solo admitía dos *hackers* a su altura. Sentía un profundo desprecio por la división informática del FBI, pero no tenía reparo en reconocer las habilidades de Max Vision, alias Iceman, pese a haber tenido algún que otro encontronazo por culpa de los ataques de Iceman contra Dark Market. En cuanto a su viejo amigo Lord Cyric, Cha0 llegaba al extremo de ponerlo por encima de sí mismo en el panteón *hacker*.

En poco tiempo, Lord Cyric había conseguido convertirse en moderador y administrador de foros como The Grifters, Carders Market y, por último, Dark Market. Nadie sabía a qué jugaba ni qué se proponía, aunque las víctimas de sus ataques estaban seguras de que trabajaba para las fuerzas del orden, ya fuera como agente o como confidente.

En Pittsburgh, el agente del FBI Keith Mularski no sabía qué pensar. Como tantos otros, creía que la persona que se ocultaba tras Lord Cyric vivía en Montreal, pero las averiguaciones de la división telemática de la Real Policía Montada resultaron infructuosas. De hecho, aunque las direcciones IP de Cyric conducían a Montreal, en ocasiones parecían apuntar también a Toronto, donde algunos sabuesos creían que residía.

Varios *hackers* creyeron y divulgaron el rumor de que Lord Cyric era en realidad Brian Krebs, un periodista especializado en seguridad informática que por entonces escribía para *The Washington Post*. No había pruebas de ello; parecía más bien lo contrario: Krebs era un profesional demasiado serio como para arriesgar su reputación mezclándose con la gente a la que investigaba. Circularon muchos rumores, pero nunca llegó a saberse quién era en verdad Lord Cyric ni cuáles eran sus intenciones.

Lord Cyric exhortaba a otros a que perpetrasen toda suerte de actividades delictivas, en tanto que él nunca llevaba a cabo ninguna, lo que reforzaba la tesis de que trabajaba para la policía o los cuerpos de inteligencia.

Lo que nadie ponía en tela de juicio era que Lord Cyric poseía un conocimiento enciclopédico de la comunidad tarjetera y su funcionamiento. Por eso todo el mundo iba detrás de él: los tarjeteros para que los pusiera en contacto con colegas de su confianza o para averiguar si tenía información relativa a ellos, y las policías de Estados Unidos y Europa occidental para

intentar reclutarlo como parte de su cruzada contra la delincuencia informática.

Cyric encarnaba la quintaesencia de la clandestinidad cibernética: aparecía como de la nada; exhibía una arrogancia ilimitada y detestable, y, sobre todo, sus motivos para dedicar horas y horas a colgar mensajes, enzarzarse en debates —a menudo fútiles— y zaherir a sus compañeros resultaban oscuros.

Hasta que Mert Ortaç descubrió que dos de los usuarios más prominentes de la embrionaria internet turca, el sistema de tablón de anuncios, se llamaban Cha0 y Lord Cyric, nadie empezó a atar cabos.

Valiéndose de su característica mezcla de encanto y falsedad, Mert —que a finales de la primavera de 2007 firmaba como PilotM— se presentó a Lord Cyric como una tercera persona, conocido común de ambos. «¡Hola, viejo! —Le escribió—. ¿Qué haces en un foro cómo este?». Cyric, perspicaz, le hizo la misma pregunta al supuesto viejo amigo. Pronto, sin embargo, empezaron a discutir sobre temas de encriptado. Mert se dio cuenta de que Lord Cyric era un ingeniero informático extremadamente brillante, lo que confirmaba sus sospechas acerca de la verdadera identidad del personaje. Tras varios días, o semanas, intercambiando ideas e información, Cyric accedió a arreglar un encuentro virtual entre Cha0 y Mert (que seguía haciéndose pasar por otra persona). Mert empezó a tratar con Cha0 vía mensajes de ICQ encriptados (y en turco, por supuesto).

«La verdad —le confesó Cha0 a Mert— es que no paso mucho tiempo en Turquía. Prefiero vivir en el extranjero». Decía que sus compatriotas no le caían muy bien y que, en la medida de lo posible, evitaba el trato con ellos. «Me llamo Şahin —dijo—, y no hablo en turco a menos que sea absolutamente necesario». Si se había dignado a hablar en turco con Mert, era porque los había presentado Lord Cyric. «Él y yo somos viejos amigos», admitió Cha0.

En abril de 2007, Cha0 había expulsado a Dron de Dark Market, por lo que se había quedado sin nadie capaz de hacerse cargo de los microprocesadores de las clonadoras. Le preguntó a Mert si sabría hacerlo, y este accedió. A partir de ese momento se convirtió en cómplice de los turbios negocios de Cha0, pero a cambio ganó algo que no tenía precio: su confianza.

Mert es la única persona que puede presumir de haber tenido trato íntimo con Cha0 y Lord Cyric, en tanto que estos no pueden afirmar con certeza si alguna vez intercambiaron mensajes con Mert, que siempre se hizo pasar por otra persona. Cha0 negó de forma explícita haber conocido o mantenido

correspondencia con él antes del fatídico día en que lo secuestró y colgó su fotografía en internet, a través de Haber 7.

Es más: nadie en Turquía ni en ningún otro lugar del mundo ha reconocido nunca la existencia del misterioso Şahin. Aparte de la palabra de Mert, no hay pruebas de la existencia de Şahin ni de un posible encuentro entre ambos. Sin embargo, Mert tenía razón en algo: la amistad entre Lord Cyric y Cha0 venía de muy lejos.

A todo esto, Mert seguía colaborando con la Agencia Nacional de Inteligencia turca, y muchas tardes, tras pasar buena parte del día fingiendo trabajar para Fox Turquía, explorando Dark Market o produciendo microprocesadores para la industria clonadora de Cha0, Mert informaba a sus contactos de los hallazgos realizados durante el día. Les habló de un *spammer* polaco llamado Master Splyntr; de Grendel, el genio de la seguridad; de Lord Cyric y Cha0; de los servidores de recuperación de que los administradores de Dark Market disponían en diferentes países europeos, y de las actividades del DHKP/C.

Pero ¿qué se traía entre manos? Su superior en Fox Turquía se fiaba cada vez menos de él. Casi nunca terminaba las tareas que se le encomendaban y siempre tenía a punto una ristra de excusas para explicar sus ausencias del puesto de trabajo. Mert afirmaba padecer una grave enfermedad, y cada dos por tres pedía dinero prestado a sus compañeros. Si tenía tanto éxito en todo, se preguntaba su jefe, ¿cómo era posible que siempre le faltase dinero?

Un día el jefe descubrió que Mert había pedido las contraseñas de todos sus compañeros. En teoría, las necesitaba para instalar una actualización importante en el sistema. El jefe, sin embargo, sospechó que Mert quería las contraseñas para fines menos honorables y frustró su plan justo a tiempo.

En otra ocasión descubrió a Mert con una pila de tarjetas de crédito encima de la mesa. Más tarde, supo que tenía dos documentos de identidad, ambos con nombres falsos y fechas y lugares de nacimiento inventados. Por último, sorprendió a Mert navegando por una web que contenía instrucciones detalladas sobre cómo abrir cajeros automáticos. Cada día que pasaba, las necesidades económicas de Mert eran mayores y alcanzaban ya cifras alarmantes.

Entretanto, Mert había conocido a Sanem, una mujer de ensueño de la que se había enamorado sin remedio. Sanem es la única persona en el mundo que puede confirmar o negar la extraordinaria historia de Mert. Sin embargo, se niega a hablar.

32

DELICIAS TURCAS

El estadio Sükrü Saracoğlu, en el bullicioso barrio asiático de Kadıköy, estaba lleno hasta la bandera para el último partido en casa de la temporada del Fenerbahçe. Como ya se sabía que el Fenerbahçe iba a ser el ganador de la Süper Lig, aquel partido, disputado un radiante domingo de finales de mayo, se había convertido en una ruidosa fiesta para su afición, una de las más apasionadas del mundo.

Mert Ortaç fue al estadio. Quizá de verdad, quizá solo en su fantasía.

En los palcos de honor se respiraba una atmósfera expectante y cordial. Şahin y su lugarteniente de confianza, Çağatay Evyapan, esperaban el comienzo del partido, a las cinco en punto de la tarde. Los hinchas de Estambul están considerados de los más fanáticos de Europa, y se dividen en tres campos. Dos de ellos, Galatasaray y Beşiktaş, se hallan en la parte europea de la ciudad, mientras que las camisetas amarillas y azul marino del Fenerbahçe son características del otro lado del estrecho, el asiático. Tanto Şahin como Çağatay eran hinchas declarados del Fenerbahçe, y las visitas de este último a la ciudad solían coincidir con algún encuentro; de hecho, tenía un abono en el palco de honor.

Entre los amigos invitados a ver el partido estaba Mert, quien, por lo que Şahin le había dicho a Çağatay, era una de las incorporaciones recientes al negocio de las clonadoras. Mert les presentó a su nueva novia, Sanem. Mert estaba ciego de amor por ella, y ella, cegada por la ostentosa riqueza de sus colegas.

Sanem conocía de antemano el currículo de algunos de los presentes en el palco. No era difícil arrancarle secretos a Mert, que era un charlatán nato y, además, se moría de ganas de impresionar a la muchacha, a la que consideraba muy por encima de su categoría. La presencia de tipos poderosos como Şahin y su fornido compinche Çağatay haciendo el gallito por el palco debía de convencer a Sanem de que el pequeño Mert estaba bien relacionado. A no ser, claro, que el episodio del partido del Fenerbahçe haya tenido lugar tan solo en la imaginación de Mert.

Al muchacho le iban bien las cosas. Él y Sadun habían empezado a ganar grandes cantidades con la estafa de Akbank; como confidente de la Agencia Nacional de Inteligencia gozaba de una amplia inmunidad, y, además, se había ganado el respeto de Cha0, el miembro más importante de Dark Market. Pero, por encima de todo, pasaba los días y las noches en compañía de una mujer fabulosa y atractiva que parecía igual de enamorada que él.

Llegó el verano y Mert decidió capitalizar su buena fortuna tomándose unas vacaciones en Antalya, en el codiciado hotel Adam & Eve, cuyos diseñadores habían logrado combinar un presupuesto elevado con un peculiar mal gusto. El hotel dispone de enormes piscinas que rodean un atrio de luces de colores, y sus habitaciones son conocidas por los innumerables espejos que invitan a pasar noches de sexo desenfrenado. Alojarse en él no sale barato. El precio mínimo por habitación es de cuatrocientos dólares por noche, y los extras suelen ascender a una buena suma. Sin embargo, para la juventud guapa y rica del país era el destino de moda de la temporada.

Nada más registrarse, Mert y Sanem se encontraron con Çağatay, que también había decidido pasar el verano en el sur. Çağatay le dijo a un tipo rechoncho con gafas que iba con él que Mert ayudaba a Cha0 con los «asuntos administrativos». El tipo rechoncho observó a Mert con gesto pensativo y exclamó: «¡Un momento! ¡Yo conozco a este tipo desde que iba en pantalón corto! ¿Qué haces metido en este negocio?». Mert, como siempre, respondió con su sonrisa maliciosa.

Mientras él y Sanem se dirigían a la habitación, Mert dijo: «¿El otro tipo? Es Lord Cyric». Sanem le preguntó si Lord Cyric era más poderoso que Cha0, y Mert le dijo que no, pero recordó una vez más que a la muchacha lo que la atraía era ante todo el poder y, después, el dinero.

Mert, en su enamoramiento, creía estar en el cielo. Era un tipo adinerado a quien respetaban tanto los delincuentes como los servicios de inteligencia. De puertas afuera, tenía un buen puesto en el departamento de tecnologías de la información de Fox Turquía, y, por si fuera poco, se disponía a pasar el verano en el Adam & Eve con una mujer de bandera. Mejor imposible.

Y es que, con la perspectiva del tiempo, agosto de 2007 marcó una breve edad de oro en el ensoñado mundo de Mert Ortaç; por una vez, sus fantasías coincidían con la realidad. En cuanto volvió a Estambul, las cosas empezaron a escapársele de las manos y, con la llegada del otoño, se inició un periodo oscuro. Sanem y Mert adquirieron la costumbre de realizar costosos viajes de compras a lugares como la isla de Míkonos, en la vecina Grecia. La pareja podía llegar a gastarse miles de euros en un solo día, un desembolso excesivo

incluso para una cartera tan llena como la suya. Mert empezaba a cansarse de la tendencia de su novia al despilfarro, y ella, de sus secretos y mentiras.

Poco después, Mert fue detenido bajo la confusa acusación de haber sustraído cinco mil euros a un amigo del hermano de Sanem. Para Fox Turquía, aquella detención era la gota que colmaba el vaso, así que lo despidieron. Por si fuera poco, la Agencia Nacional de Inteligencia decidió que Mert se había convertido en un lastre que no valía la pena seguir soportando. De un día para otro, Mert se quedó totalmente desprotegido y sin dos importantes fuentes de ingresos.

Tras quedar en libertad bajo fianza, retomó el negocio de las tarjetas con Sadun gracias a las continuas vulnerabilidades de los sistemas de Akbank. Su inquietud se convirtió en desesperación al enterarse de que Sanem tenía un amante. La ruptura entre ambos se tradujo en un episodio tempestuoso rematado por un doloroso cruce de acusaciones. Mert creía que ella le había robado grandes sumas de dinero, y ella, a buen seguro, debió de pensar que se había vuelto loco.

Al ver que el mundo se tambaleaba bajo sus pies, Mert decidió empezar el año con un viaje al sur para meditar sobre su futuro. Por el camino, siguió recibiendo malas noticias: Sadun había sido detenido y la policía había registrado el piso de Mert con una orden de detención. De haberse quedado en Estambul, a esas alturas ya lo habrían puesto entre rejas. Como de costumbre, ante la adversidad, Mert decidió esconder la cabeza en el suelo y buscar el modo de desaparecer.

Tras regresar a Estambul con un nombre supuesto, empezó a tramar un plan de huida. Con uno de sus documentos de identidad falsos, solicitó —y consiguió— un pasaporte nuevo y sobornó a un funcionario del consulado francés a fin de obtener un visado. Acto seguido emprendió un tortuoso viaje: del territorio francés de la Martinica, en el Caribe, pasó a París y, finalmente, a Alès, una apacible población ochenta kilómetros al norte de la costa mediterránea de Francia.

Mert estaba aislado. Sus recursos eran limitados, apenas hablaba una palabra de francés y, lo que era peor, no disponía de acceso a internet. Por lo menos podía consolarse pensando que se encontraba a salvo. Así pues, incapaz de otra cosa, Mert se sumió en un largo periodo de descanso y relajación.

Después de la angustiosa experiencia como prófugo de la justicia turca y de la pelea con su exnovia, Alès no tardó en parecerle un agradable lugar de retiro. Por primera vez en muchos meses, tal vez años, podía olvidarse de las

medias verdades, los engaños, los robos y las prevaricaciones. Podía poner fin a la rígida compartimentación que exigían sus múltiples personalidades reales y virtuales y buscar su auténtica esencia; suponiendo, claro está, que la conservara. Quizá había llegado el momento de acabar con aquella locura; quizá era hora de enmendarse, buscarse un trabajo de verdad y sentar la cabeza junto a un mujer decente. Si jugaba bien sus cartas, todavía estaba a tiempo de hacerlo.

De pronto, una mañana hacia las ocho, alguien llamó a la puerta.

Mert estaba tendido en la cama sorbiendo un café. Hasta entonces, en Alès no había recibido visitas, y tampoco las esperaba. Se puso una bata, se dirigió hacia la puerta y, al abrir, se encontró con dos hombres cargados con sendas mochilas. «¡Hola, Mert! ¿Qué tal estás?», dijo el primero en turco. Mert respondió murmurando: «*Je ne comprends pas…*». «Vamos, Mert —intervino el segundo en inglés—. Sabemos quién eres. Lo mejor para ti es que nos invites a pasar».

Tras tomar asiento en la cocina frente a una taza de café, uno de los hombres sacó una carpeta y la puso sobre la mesa. Mert pensó que debía de ser un norteamericano de segunda generación con raíces turcas, pues, aunque hablaba un turco coloquial, tenía algo de acento y cometía algún que otro error gramatical. El otro, que fue quien habló la mayor parte del tiempo, era estadounidense.

A Mert le ofrecieron dos opciones: «O nos prestas ayuda incondicional, o le entregamos esta carpeta a la Sécurité». Mert echó un vistazo a unos folios donde figuraban tarjetas de crédito francesas que él y Sadun habían clonado al introducirse en las tripas del sistema informático de Akbank. Los dos hombres le recordaron que en Francia podían condenarlo a ocho años de prisión por un solo caso de fraude con tarjeta de crédito.

No tenía alternativa. Pero, antes de asentir, Mert quiso saber a quién representaban los dos hombres. Le dijeron que a las fuerzas de seguridad estadounidenses. «¿Y qué queréis de mí?», preguntó Mert.

«Vamos, Mert, ¡adivina!».

Mert, furioso y asustado, sacudió la cabeza.

«Queremos que nos entregues a Cha0».

33

REGRESO AL HADES

Durante el rato que pasaron hablando sobre Cha0 y su posible paradero, Mert cayó en la cuenta, por sus preguntas y comentarios, de que no conocían ni la identidad de Cha0 ni la de Lord Cyric. Los agentes le informaron de que tendría que regresar a Turquía, volver a ingresar en Dark Market y desencovar a Cha0 y sus colegas. Su sorpresa fue todavía mayor cuando los agentes añadieron que uno de los suyos tenía controlado el servidor de Dark Market. De esa forma, podrían facilitarle de nuevo el acceso a los foros.

Por lo que Mert podía colegir, parecía que el FBI había decidido ir a por el resto de los miembros importantes de Dark Market: Cha0, Lord Cyric, Master Splyntr, Shtirlitz y Grendel. No le dijeron cómo exactamente, pero era evidente que le habían reservado un papel decisivo en aquella operación. La idea no lo seducía, pero tampoco la posibilidad de pasar una temporada en una de las prisiones francesas, que por lo que se rumoreaba eran las más duras de toda Europa occidental.

Los agentes le hicieron unas cuantas promesas más bien vagas y le facilitaron el número de teléfono y la dirección de correo electrónico de Lucy Hoover, la asistente jurídica agregada a la embajada estadounidense de Estambul. Asimismo, le abrieron una cuenta de correo (sadinsider@gmail.com; el nombre lo eligió el propio Mert) a través de la cual podría ponerse en contacto con ella.

La estancia de Mert en el Languedoc es el segundo episodio no verificable de su mundo onírico. Lo que sí es cierto es que se puso en contacto con Lucy Hoover, del FBI, que por entonces estaba destinada en Estambul.

Mert llevaba dos meses fuera del país a su regreso el 2 de marzo de 2008. Lo primero era trazar un plan de actuación. Decidió tantear a Haber 7, la agencia de noticias y cadena televisiva turca, ofreciéndoles una entrevista en la que prometía revelar algunos secretos acerca de Dark Market y el mundo del tarjeteo. Es posible que su intención fuera poner sobre aviso a Cha0, hacerle saber que se había filtrado información acerca de sus actividades y que la policía tal vez estuviera investigándolo.

En su inocencia —que, pese a todo, seguía siendo parte integral de su carácter—, Mert supuso que Cha0 no sabría quién era en realidad el misterioso *hacker* que ofrecía aquella entrevista a la prensa. Con lo que Mert no contaba era con que Haber 7 sacaría una imagen a escondidas de él en el McDonald’s de Kadıköy, donde se había reunido con el periodista de la cadena. Al publicarse la fotografía, Cha0 supo quién se había ido de la lengua y puso a Mert bajo el punto de mira.

Cha0, Lord Cyric y compañía sabían que había una orden de detención contra Mert y que Sadun estaba en el calabozo, por lo que imaginaban que Mert era vulnerable a la presión policial. La entrevista vino a reforzar sus sospechas. En lugar de regresar enseguida a Dark Market, Mert se puso en contacto con un joven *hacker* amigo suyo llamado Mustafa, conocido también de Cha0. Mustafa se mostró encantado de poder ganar un poco de dinero fácil con el negocio de las tarjetas.

La familia de Mustafa provenía de Antalya, con lo que Mert tenía una excusa para salir de Estambul, donde se sentía inseguro. Se quedó en el sur, su parte favorita del país, algo más de un mes.

Mustafa empezó a operar en Dark Market con el alias MYD y trabó una buena relación profesional con Cha0. Lo que Mert no sabía era que Mustafa le había advertido a Cha0 que Mert parecía querer traicionarlo.

Mustafa concertó una reunión con Cha0 en Estambul en cuanto él y Mert regresaron al norte. Mert mantenía a Lucy Hoover informada de todos sus movimientos y la alertó de que pronto se reuniría con Cha0. Los estadounidenses necesitaban identificar a Cha0 y determinar cuáles eran sus coordenadas y su infraestructura comunicativa. Por una vez, Mert había sido fiel a su palabra: estaba conduciendo a los norteamericanos hacia su presa. Cha0 había dado instrucciones a Mustafa para encontrarse frente a un Burger King en las proximidades de la estación de metro de Göztepe, en la parte asiática de Estambul, a unos tres kilómetros del estadio del Fenerbahçe.

Cuando llegaron a Göztepe se encontraron con Hakan Öztan, un tipo fuerte como un toro que había sido el guardaespaldas de Çağatay durante el paso de ambos por prisión y que ahora ofrecía sus servicios también a Şahin. El guardaespaldas los condujo hasta un edificio con el rótulo «Apartamentos Sözdener», en el distrito de clase media acomodada de Suadiye, a unos tres kilómetros. Las habitaciones estaban escasamente amuebladas y no eran especialmente acogedoras. Hakan les dijo a los dos hombres que esperasen, que alguien vendría a buscarlos.

No contaban ya con la protección de los espacios abiertos, y menos de la Agencia Nacional de Inteligencia. Mert empezaba a temer que Çağatay quisiera ajustar cuentas con él. Sin él saberlo, Mustafa, a instancias de Cha0, había instalado en su portátil un virus troyano que permitía a Cha0 conocer todos los secretos de Mert y, por consiguiente, también su doble juego. Cha0 no era tan solo un criminal experimentado, sino también un tipo vengativo. Ahora poseía pruebas sólidas de que Mert estaba trabajando para la policía. Mert suponía (o al menos esperaba) que Lucy Hoover debía de tener el apartamento bajo vigilancia de algún tipo, pero no era así, de modo que si Çağatay, Şahin, Haktan o los tres aparecían por ahí, estaría metido en un buen lío.

Cuando el timbre sonó el domingo 18 de mayo de 2008 a las diez en punto de la mañana, Mert estaba solo en los apartamentos Sözdener. Al abrir, se encontró con Haktan. Sin mediar palabra, el visitante pasó y cerró la puerta. Con voz alegre, Mert comentó que lo estaba esperando. Haktan se quedó mirándolo y dijo: «Espera». Entonces abrió la puerta y entró Çağatay. Mert, hasta ese momento sonrojado, se quedó lívido y, finalmente, palideció.

Çağatay lo obligó a sentarse en una silla y se puso a caminar despacio de un lado a otro delante de él, repitiendo: «*Mert… Namert… Mert… Namert…*», un juego de palabras, ya que en turco la palabra *mert* («valiente») es antónima de *namert* («cobarde»).

Al momento siguiente, Mert estaba en el suelo recibiendo patadas en el estómago, el pecho y las piernas. Entraron otros dos matones, que le taparon la cabeza con una manta para que no pudiera reconocerlos y se sumaron a la paliza. De vez en cuando, a Mert le parecía ver una pistola apuntándole a la cabeza.

Se desmayó. Cuando volvió en sí, seguía tendido en el suelo. Reparó en que había una cámara de vídeo grabándolo todo. Al instalar el troyano en el portátil de Mert, Cha0 había descubierto datos relativos no solo a su relación con Lucy Hoover, sino también a sus contactos en la Agencia Nacional de Inteligencia (de la que no había salido del todo bien parado).

«Muy bien —dijo Çağatay, que ejercía de maestro de ceremonias—. Ahora nos vas a contar toda la historia, desde el principio hasta el final». Mert estuvo hasta las tres de la madrugada explicándoles su historia de espías. Querían saberlo todo —sobre los agentes infiltrados, sobre los negocios con Sadun, sobre la exploración de Dark Market, sobre su novia—, hasta el último detalle.

Los matones se fueron por fin a dormir, a excepción de uno, que se quedó despierto, y cada vez que veía que Mert movía la cabeza, avisaba a los demás para regalarle una nueva lluvia de puñetazos y puntapiés.

El lunes a mediodía, Şahin telefoneó y Çağatay le pasó el aparato a Mert. Para entonces, el muchacho no podía ni tenerse en pie. Estaba convencido de que iban a matarlo, así que no se sorprendió cuando Şahin le dijo que repitiera su declaración. Quedó todo grabado. Cuando hubo terminado, Şahin tomó de nuevo la palabra: «Muy bien, ahora ha llegado la hora de tu castigo —dijo sin ironía—. Quiero que hagas todo lo que te diga Çağatay. Luego veré qué hago contigo».

Çağatay le dijo que se levantase y se quitara la ropa. Mert, que temió que fueran a violarlo en grupo, imploró: «Por el amor de Dios, metedme una bala en la cabeza. ¿Se puede saber qué vais a hacer conmigo?».

«Cállate —replicó Çağatay—, no tienes por qué preocuparte. No somos una panda de sodomitas. ¡Déjate puestos los calzoncillos y acepta tu castigo!». Por teléfono, Şahin le dictó a Çağatay la infamante nota que señalaba a Kier, o Mert Ortaç, como traidor y soplón. Así fue como nació la leyenda de Kier. El periodista de Haber 7 había encontrado el nombre de Mert en una web junto al alias de Kier, pero Mert en realidad nunca había utilizado —ni utilizaría— ese nombre; su verdadero alias era SLayraCkEr. Sin embargo, después de la fotografía que le tomó Çağatay, periodistas, policías y tarjeteros del mundo entero empezaron a referirse a Mert Ortaç como Kier, a pesar de que nadie lo había llamado así nunca.

Tras la sesión fotográfica, volvieron a arrojar a Mert al suelo y le echaron una manta encima. «Espera aquí media hora. Después puedes marcharte —dijo Çağatay—. Te hemos dejado tu ropa y el dinero. También puedes quedarte con uno de los documentos de identidad. En adelante, y durante el resto de tu vida, ni se te ocurra volver a escribir el nombre de Cha0, porque, si lo haces, te encontrarás con mis manos rodeándote el cuello antes de que puedas volver a tomar aire». Çağatay no pudo resistir la tentación de añadir un toque personal: «Por mí, te habría matado aquí mismo. Pero le caes bien. Sé agradecido y mantén la boca cerrada». (Çağatay, en realidad, se tomaba a risa que alguien pudiera pensar que deseaba matar a un fracasado como Mert).

Media hora después, el maltrecho Mert Ortaç, con solo cincuenta dólares en el bolsillo, salió tambaleándose del apartamento y se dirigió a la estación de autobuses nacionales, donde tomó uno con destino a Esmirna. Allí se lamería las heridas y pensaría qué demonios hacer. Era evidente que debía pasar a la clandestinidad. Así pues, Mert desapareció por última vez… hasta

su arresto unos meses más tarde al solicitar un pasaporte con nombre falso en noviembre de 2008.

El mundo onírico de Mert —entre la realidad y la fantasía— abunda en muchos otros relatos igual de extravagantes pero, para nuestro propósito, podemos terminar aquí.

34

DESCABEZAR AL TURCO

Antes de que Mert fuera por fin detenido, el inspector Bilal Şen no tenía la menor idea de si se hallaba fugado, preso o sencillamente muerto. Lo que sí sabía era que el tiempo no jugaba a su favor. Lo único que podía hacer el agente era seguir tras la pista de Cha0 con toda la diligencia y paciencia posibles. Ahora al menos disponía de la fotografía y el teléfono del remitente de la clonadora, y estaba convencido de que eso terminaría conduciéndolo hasta Cha0. Gracias a que el esbirro que había entregado la clonadora utilizaba uno de los números consignados en la empresa de mensajería, la policía pudo «triangular» al sujeto; es decir, que lograron identificar a qué antenas telefónicas se conectaba el aparato. No tardaron en hacerse una idea exacta de su situación y de sus movimientos habituales.

Poco después volvieron a avistarlo y empezaron a seguirlo. A los pocos días, el tipo los condujo hasta una finca de Tuzla, un suburbio de Estambul situado unos veinticinco kilómetros hacia el sur siguiendo la costa asiática. Sede de una de las mayores bases navales de Turquía, la zona, famosa por la pesca, era de las pocas en la ciudad que no había sido conquistada por edificaciones de nueva planta. La espaciosidad de las casas y el colorido de los exteriores lo convertían en un barrio muy cotizado, habitado sobre todo por familias pudientes.

El sospechoso los condujo hasta una lujosa villa con piscina. Tras varios días de observación, el equipo de vigilancia determinó que en la villa vivían varios hombres. Bilal no tardó mucho en averiguar quién daba las órdenes. Al revisar expedientes, dio enseguida con el de Çağatay Evyapan.

En la universidad, Çağatay había sido un buen estudiante de ingeniería eléctrica. En 1998, había sido detenido por estafa. Dos años después, cometió el error de su vida: fue detenido, junto a dos colaboradores, por retirar dinero en los cajeros automáticos del puerto de Esmirna con tarjetas de crédito clonadas. A los cinco años de prisión —de un total de veintisiete—, la idea de seguir encerrado se le hizo insoportable. Un día, en mayo de 2005, Çağatay

escaló los muros de la cárcel y eludió el radar. Más que un fugitivo, parecía un fantasma.

Culpaba de su arresto a los tipos con los que trabajaba, y juró que no volvería a sucederle. La filosofía de Çağatay podía resumirse en lo siguiente: «Si quieres que las cosas salgan bien, hazlas tú mismo».

Sabía que, durante los cinco años que había pasado en prisión, el mundo cibernético debía de haber experimentado cambios sustanciales. Conocía bien la ley de Moore, según la cual el número de transistores aplicables a un circuito integrado se duplicará cada dos años hasta 2015. Trasladada al mundo real, significa que cada año los aparatos son más complejos; los programas informáticos, más enrevesados; las herramientas de los *hackers*, más precisas, y las recompensas, por lo tanto, más jugosas. Consciente de todo ello, empezó a adaptarse a las nuevas circunstancias.

Ante todo, necesitaba una nueva identidad cibernética. Çağatay desapareció durante casi cuatro años; el nombre de su pasaporte se convirtió en el de uno de sus subordinados, el guardaespaldas Hakan Öztan, y en la red pasó a ser Cha0 (pronúnciese como el saludo italiano). Utilizaba la primera sílaba de su nombre y el número cero desde su primera toma de contacto con los BBS en los años noventa. Por entonces, el excepcional sistema de seguridad de Cha0 había impedido que nadie lo identificara. En foros públicos como Crime Enforcers y Dark Market, Cha0 vendía clonadoras. En privado, vendía sistemas de seguridad impenetrables a usuarios informáticos que no podían permitirse revelar su identidad.

Sin embargo, ahora Bilal había dado con él. De todos modos, una cosa era localizar el paradero de Cha0, y otra recabar las pruebas pertinentes para incriminarlo. La judicatura y la fiscalía turca poseen un grado de conocimiento de internet menor que el de sus homólogos en Europa occidental y Norteamérica, y de hecho ya eran varios los abogados defensores de alto nivel que sabían cómo aprovechar esa ignorancia en beneficio de sus clientes y de sus propios honorarios.

Çağatay estaba disfrutando del verano; era un tipo sociable al que le gustaba divertirse con sus amigos. A menudo se dejaba ver en compañía de mujeres atractivas, entre ellas, se rumorea, una atrevida integrante de la familia real saudí. Le gustaban las bebidas caras, la buena comida y las fiestas en yates. Con los años había ganado algo de peso. El dinero parecía lo de menos en su búsqueda de un estilo de vida sofisticado.

Bilal mandó seguir a varios de los colegas de Çağatay: las pruebas empezaban a sugerir que Cha0 no solo era Çağatay Evyapan, sino una

organización delictiva bien cohesionada. Se enfrentaban a un grupo criminal, no a un mocoso inexperto que jugaba a piratear servidores. Por lo demás, parecía tratarse de una tendencia en aumento en todo el mundo. Durante muchos años, las organizaciones criminales apenas habían prestado atención a la delincuencia en la red por parecerles inofensiva, pero eso estaba comenzando a cambiar. La delincuencia telemática era cada vez más sistemática, eficaz y segura, y empezaba a salir de la incubadora —frecuentada por *geeks* con ganas de jugar y divertirse— para entrar en un terreno más adulto: el de las estructuras mafiosas. Por todo ello, era de suponer que la presa de Bilal dispusiera de importantes recursos; el inspector tendría que emplearse, pues, al máximo para presentar cargos y evitar que los tribunales los desestimasen.

La policía empezó a reunir pruebas. Keith Mularski siguió administrando Dark Market mano a mano con Cha0. La operación duró cinco meses largos, durante los cuales el archivo de pruebas de Bilal fue aumentando poco a poco. Averiguó que el círculo íntimo de Çağatay era relativamente reducido y que sus medidas de seguridad eran de una precisión casi militar. Aparte de las pruebas —con las que habría podido relacionar a Çağatay con cualquier tipo de delito—, existía otro frente abierto: faltaba saber si Çağatay tenía un topo; era de esperar que no.

A finales de agosto, Çağatay se esfumó. En el equipo de seguimiento cundió el pánico. No obstante, el periodista de Haber 7 seguía recibiendo mensajes, no de Cha0, sino de un tal Yarris, que parecía conocer muy bien las actividades de Cha0. Por suerte para Bilal, Cha0 reapareció en Estambul tan inesperadamente como se había evaporado. Esto podía interpretarse como un signo de la precariedad de la situación. Así las cosas, Bilal decidió fijar la fecha de su detención para principios de septiembre.

El equipo de vigilancia sabía que uno de los residentes en la villa de Tuzla salía cada pocos días para comprar provisiones. El 8 de septiembre salió de la casa. Bilal Şen estaba en Ankara mordiéndose las uñas, mientras la unidad de intervención especial, que tenía rodeado el edificio, lo informaba por teléfono de los acontecimientos minuto a minuto. Al regresar el proveedor, se dio orden de intervenir: la policía entró en la finca y detuvo a cuatro personas. En el lugar había una gran cantidad de ordenadores, docenas y docenas de clonadoras, moldes, teclados, datáfonos y mucho dinero en efectivo. La operación fue un éxito; nadie resultó herido y todos los sospechosos fueron detenidos.

Curiosamente, la detención de Cha0 había sido anunciada pocos días antes en los foros de la revista *Wired*, después de que uno de los redactores publicara un artículo sobre Dark Market en la web de la revista. Uno de los últimos comentarios lo firmaba alguien que afirmaba ser Lord Cyric, el administrador de Dark Market. Aseguraba que mantenía contacto directo con Cha0 y, con palabras algo crípticas, daba a entender que tal vez algunos de los subordinados de Cha0 darían algún día con sus huesos en prisión, pero que Cha0 no caería jamás.

¿Adiós, Cha0?

35

LA MUERTE DE DARK MARKET

Quienquiera que fuera Cha0 realmente, la inesperada detención de Çağatay Evyapan sembró el pánico entre los demás administradores de Dark Market. El 16 de septiembre de 2008, menos de una semana después de la redada de Estambul, Master Splyntr anunció en la web que los éxitos de la policía estaban acabando con los nervios tanto de él como de los demás administradores. Ninguno de ellos se sentía capaz de seguir soportando aquella carga:

> Resulta evidente que este foro […] ha atraído demasiado la atención de muchos cuerpos de todo el mundo (agentes del FBI, el Servicio Secreto y la Interpol). Supongo que era cuestión de tiempo que ocurriera. Lamento que se haya llegado a esta situación, porque […] hemos logrado convertir a DM en el foro de negocios líder en lengua inglesa. Pero así es la vida. Cuando llegas a la cima, la gente intenta derribarte.

La principal web criminal del mundo anglófono moría en solo una semana. Sus seguidores estaban consternados: «Dark Market era nuestro puente para los negocios, y si ese puente cae…», se lamentaba un miembro llamado Iceburg en un mensaje colgado en la web de la revista *Wired*. «Vivan el robo y las tarjetas. Mueran las RATAS y el FBI y todos los malditos organismos secretos que no solo traen la ruina a nuestra vida y nuestras familias, sino que destruyen todo lo que habíamos construido».

Daba la impresión de que los ciberpolicías habían ganado. Aunque, tratándose de Dark Market, las cosas no podían ser tan fáciles.

PARTE IV

36

DOBLE TRAICIÓN

Stuttgart, septiembre de 2007

Al agente Dietmar Lingel le encantaba su trabajo. La semana anterior, su superior le había entregado los registros del proveedor de mensajería electrónica canadiense Hushmail. En teoría, el sistema de mensajería de la empresa era hermético y garantizaba que nadie pudiera acceder a la correspondencia de sus clientes. Hasta cierto punto, la teoría era cierta, pero en 2007 la compañía cedió a las presiones de la policía canadiense y permitió que las fuerzas de seguridad consultaran sus registros, que revelaban desde qué direcciones IP se había consultado una determinada cuenta de correo. La Real Policía Montada del Canadá envió al agente Mularski del FBI los registros relativos a dos cuentas: auto432221@hushmail.com y auto496064@hushmail.com.

En mayo de 2007, Matrix001 le había enviado a Keith Mularski una versión editada de los correos anónimos en los que se le avisaba que estaba bajo la vigilancia de la policía alemana. En un primer momento, Mularski creyó que la filtración procedía de sus colegas del Servicio Secreto. Por entonces, federales y Servicio Secreto tenían abiertas investigaciones independientes sobre Dark Market, lo que multiplicaba las posibilidades de que se abriera una brecha de seguridad, ya fuera por incompetencia o por malicia. Sin embargo, por lo menos otras tres fuerzas policiales tenían conocimiento de la existencia de Matrix: las de Gran Bretaña, Francia y, por supuesto, Alemania.

Nadie subestimaba la importancia de aquellos mensajes. Además de la probable existencia de un topo, cabía la posibilidad, igualmente inquietante, de que alguien hubiera pirateado los ordenadores de alguna de las unidades de la investigación. La operación Dark Market empezaba a ir en serio, y las detenciones de Matrix001 y JiLsi no eran más que el principio; la intención era mantenerla abierta durante los años siguientes. Sin embargo, los mensajes ponían en peligro la estrategia urdida a lo largo de dos años de minucioso

trabajo. Había que acabar con las filtraciones. La localización de la fuente se convirtió en el objetivo prioritario de todos los cuerpos implicados en la investigación.

Con la llegada de los registros de Hushmail a la mesa de Lingel, podía comenzar el examen detallado de las pruebas. Como especialista técnico del equipo de investigación dedicado a Matrix, Lingel era el encargado de dilucidar quién había intentado acceder a aquellas cuentas durante los días en que el *hacker* había recibido los mensajes.

Lingel vio que una de las direcciones IP desde las que se había intentado acceder a las cuentas anónimas provenía de la zona de Stuttgart. La descartó de inmediato, pues era la suya. Cuando Keith Mularski había avisado a Stuttgart de la existencia de los correos, Lingel había intentado entrar en las cuentas de Husmail utilizando algunas contraseñas típicas («admin», «password») y otras pertenecientes a miembros prominentes de Dark Market conocidas por la policía. Los demás intentos de conexión provenían de direcciones IP de Berlín y otros puntos del país. La mañana del 12 de septiembre, durante una conversación con Gert Wolf, su superior en el departamento, Lingel explicó que todavía no tenían ningún sospechoso, pero que habían conseguido acortar la lista de candidatos.

Después del almuerzo, Wolf se asomó al despacho de Lingel para decirle que tenían que ir a ver al jefe de división. Al llegar al lugar de la reunión, Lingel se encontró con un grupo de oficiales esperándolo, entre ellos un agente del temible Dezernat 3.5, el departamento de asuntos internos de Stuttgart. Su presencia desconcertó a Lingel, que se puso algo nervioso. De pronto, el agente dijo: «Señor Lingel, le anunciamos que se abre una investigación contra usted por haber avisado presuntamente a un sospechoso de que se hallaba bajo vigilancia».

Lingel se quedó sin habla. Poco a poco, el asombro dio paso a la indignación: «Me paso toda la semana trabajando mano a mano con mi jefe para resolver este lío —pensó—, y de pronto un día se asoma a mi despacho después de comer y me clava un cuchillo por la espalda».

«Veamos, señor Lingel —continuó el agente—, tiene dos opciones. O bien colabora con nosotros en esta investigación, o bien lo ponemos ahora mismo en custodia preventiva».

Lingel aceptó colaborar. Su jefe le dijo que se tomara los días de permiso que todavía le quedaban; luego quedaría suspendido hasta nueva orden.

A sus cuarenta y tantos años, Lingel era un tipo con una biografía fuera de lo corriente. Había nacido en Windhoek, la capital de Namibia, que, bajo el

nombre de África del Sudoeste, había sido uno de los pocos puestos avanzados de la Alemania imperial durante la época de las colonias. A los cinco años, se había mudado con sus padres a Ciudad del Cabo, donde se crio hablando inglés y alemán. Regresó a la tierra natal de sus padres para cursar estudios y, tras licenciarse, ingresó en la policía, en la división motorizada, donde fue ascendiendo escalafones pese a no resultarle un trabajo especialmente atractivo.

Recobró la ilusión al saber, en 2001, que se convocaba una plaza para la policía de Baden-Württemberg. El cuartel de Stuttgart necesitaba a alguien con experiencia en Linux, un sistema operativo de código abierto, para velar por la seguridad de la red. Cinco años después, obtuvo el permiso necesario para trasladarse, con sus habilidades informáticas, al departamento de investigación criminal, donde empezó a trabajar a las órdenes de Frank Eissmann.

Matrix001 no era el único ciudadano alemán identificado por Keith Mularski como miembro activo de Dark Market. Los otros dos eran Soulfly, cuyo verdadero nombre era Michael Artamonow, y Fake, que en realidad se llamaba Bilge Ülusoy. En un principio, la fiscalía del Estado intentó acusar a Matrix001 de conspiración, pero para ello había que demostrar que estaba confabulado con los otros dos *hackers*.

Por alguna razón, no obstante, nunca llegó a abrirse ninguna investigación contra Fake y Soulfly, en parte por culpa de un juez que en octubre de 2007 obligó a la fiscalía a retirar los cargos de conspiración y rebajar la acusación a la de delito de fraude con tarjeta de crédito. El motivo para evitar una investigación contra los dos presuntos conspiradores sería solo el primero de los muchos enigmas sin respuesta que acabaron minando la confianza en la capacidad de las policías provincial y federal de Alemania para hacerse cargo del caso.

Además, la policía de Baden-Württemberg en Stuttgart se jugaba mucho en la investigación de Matrix001. Generalmente, todas las comunicaciones de los casos internacionales como aquel pasaban por Wiesbaden, pero el jefe de la investigación, Frank Eissmann, había logrado convencer a sus superiores para que lo autorizaran a mantener comunicación directa con Keith Mularski, el hombre clave del FBI.

De aquí que todo el mundo sintiera un escalofrío al saber por Mularski que Matrix001 había recibido un mensaje anónimo desde una cuenta de Hushmail en el que se lo advertía de los preparativos para su detención. Las

policías de Londres, Pittsburgh y Stuttgart cruzaban los dedos con la esperanza de que la fuente no fuera ninguno de sus hombres.

La detención de Lingel supuso un alivio para los investigadores; por lo visto, habían capturado a su hombre. Sin embargo, en diciembre de 2007, el Dezernat 3.5 remitió una carta a Lingel en la que se le informaba que no habían aparecido nuevas pruebas que lo relacionaran con el envío de los correos y que podía reincorporarse al servicio al mes siguiente, a principios de 2008. Lingel, de todos modos, no regresó al Departamento IV, el que llevaba la investigación de Matrix001. Estaba demasiado dolido con Frank Eissmann, su superior inmediato, quien por lo visto era parcialmente responsable de haber inculpado a su subordinado.

Según se acercaba el juicio de Matrix, a finales de la primavera, el ambiente en los cuarteles policiales de Stuttgart era cada vez más lúgubre y proclive a la discordia. La fiscalía sabía que, si no podían presentar cargos de conspiración contra Matrix, sería difícil obtener una sentencia de prisión. Por lo demás, seguían sin saber cuál era la fuente de las filtraciones.

Pese al resentimiento de Lingel por lo ocurrido, su incorporación al Departamento I fue satisfactoria, y el comportamiento de los compañeros hacia él, ejemplar. Tras meses de miradas recelosas, aquello suponía un alivio y un cambio para mejor.

En marzo de 2008, Lingel fue nuevamente detenido. Esta vez, la acusación no era haber enviado mensajes a Matrix, sino haber puesto en peligro la identidad secreta del agente del FBI Keith Mularski.

37

EL ZORRO SIN MÁSCARA

En junio de 2008, mientras tenía lugar el juicio de Matrix, Kai Laufen, un periodista radiofónico, hojeaba un ejemplar de *Technology Review*, publicada por el MIT[2], donde dio con un artículo sobre delincuencia informática. Hasta entonces, aquel periodista de investigación de Karlsruhe, en el sudoeste de Alemania, no tenía la menor idea de que el problema estuviera adquiriendo tal magnitud. Sintió curiosidad y decidió averiguar hasta qué punto Alemania se veía afectada por delitos de ese tipo.

Investigador cauteloso y metódico, Laufen comenzó buscando los artículos del código penal alemán relativos a la delincuencia telemática. Una vez localizados, escribió por correo electrónico a una cincuentena de tribunales municipales y de distrito de todo el país para preguntarles si tenían algún caso de ese tipo entre manos.

Recibió solo un par de respuestas, una de ellas referente a un caso de fraude con tarjetas de crédito instruido en el juzgado de Göppingen, un pequeño municipio de Baden-Württemberg a pocos kilómetros de donde vivía Laufen. Un joven llamado Detlef Hartmann se hallaba en espera de sentencia acusado de trece delitos de clonación de tarjetas de crédito.

El caso no parecía revestir particular interés, pero Laufen quiso ponerse en contacto con la policía provincial de Stuttgart de todos modos. Poco después, el inspector Frank Eissmann lo ponía al corriente de las características básicas de la delincuencia informática. De pasada, mencionó que el FBI había colaborado con el Departamento IV en la investigación sobre Hartmann.

El 2 de julio, al día siguiente de que Detlef fuera suspendido por un periodo de diecinueve meses, Kai le escribió solicitando una entrevista, que curiosamente le hizo llegar por correo ordinario. Detlef y sus padres rechazaron las primeras aproximaciones del periodista, pero al cabo de tres meses transigieron. A principios de octubre, Kai se sentó frente al joven ante una taza de café.

Kai Laufen no era ningún novato. Nacido en el norte de Alemania, había pasado parte de su juventud en Brasil y se manejaba con fluidez en portugués, español e inglés. Había trabajado por toda Sudamérica y tenía ciertos conocimientos acerca del crimen organizado, pero no pudo dar crédito a lo que oía cuando Detlef empezó a explicarle la historia de Matrix001 y de sus aventuras en el mundo virtual, donde todo el mundo usaba nombres de lo más peculiares, se comunicaba en un inglés híbrido —con elementos de la jerga gansteril, anarquista y tolkeniana— y traficaba con datos bancarios robados.

Kai no tardó en comprender el alcance de aquel nuevo tipo de delitos. Con la ayuda de internet, los malhechores podían delinquir a miles de kilómetros de distancia y perjudicar a multitud de víctimas anónimas que no siempre llegaban a descubrir que su intimidad había sido vulnerada y su dinero e identidad, usurpados.

Sin embargo, si tan fácil era, se preguntaba Kai, ¿cómo habían conseguido arrestar a Detlef? «Muy sencillo —respondió este—. Uno de los administradores, con el que trabajé durante muchos meses, era un agente del FBI. Me siguió la pista y dio aviso a la policía alemana». El periodista pensó que el joven quizá sobrestimaba su propia importancia, así que le preguntó si disponía de pruebas documentales que lo demostrasen. «Sí —contestó Detlef —. Se las enviaré».

Días después, Detlef le envió a Laufen el escrito de la fiscalía en que se describía la acusación contra el joven, redactado en la inimitable jerga judicial alemana:

> Según lo demostrado en el *dossier* de la investigación, el administrador que en definitiva poseía control total sobre todas las decisiones al menos desde junio de 2006 era el agente del FBI Keith Mularski, quien se había ofrecido a hospedar el servidor a fin de reunir información más detallada concerniente a compradores y vendedores. Remitimos al documento del caso 148, archivo 1, en que Keith Mularski informa al agente investigador de la policía regional Frank Eismann [sic] lo siguiente: «Master Splynter [sic] soy yo». Que el usuario Master Splynter [sic] gestionaba el servidor queda demostrado en virtud del documento del caso 190, correo electrónico de Keith Mularski con fecha del 9 de marzo de 2007: «Me han pagado por el servidor».

Kai estaba tan estupefacto que releyó la frase: «Master Splynter soy yo». No se trataba tan solo de que Detlef Hartmann tuviera razón al decir que el FBI había seguido su pista digital, sino que fiscalía nombraba al agente por su nombre y por su alias. Fin del misterio: Kai Laufen acababa de descubrir la verdad acerca de uno de los ciberpolicías más prominentes del mundo. Tres meses antes apenas había oído hablar de la delincuencia telemática.

Kai telefoneó a la Alianza Nacional para la Formación en Informática Forense en Pittsburgh y enseguida consiguió que le pasaran con Keith Mularski, que lo atendió con su tono de complacencia habitual. Sin embargo, cuando el periodista leyó la frase del correo electrónico —«Master Splynter soy yo»—, se hizo el silencio al otro lado de la línea. Keith sabía que lo habían descubierto. La parte positiva era que quien lo había descubierto era un periodista radiofónico del sudoeste de Alemania, por lo que cabía la posibilidad de que, pese a estar en la era de internet, la noticia no traspasase las fronteras de Baden-Württemberg. Aunque, en el fondo, sabía que era una posibilidad remota.

Otra vez cabía preguntarse quién tenía la culpa de la famosa filtración.

Kai Laufen ignoraba que la policía de Stuttgart hubiera suspendido por segunda vez a Dietmar Lingel. Esta vez el motivo de la suspensión era que el agente había cedido de forma intencionada el nombre y alias de Mularski a la fiscalía para incluirlos en el expediente del caso. El objetivo de Lingel, según se alegó, era sacar la identidad de Mularski a la luz pública con el fin de desacreditar al FBI. El móvil, según la investigación, era la insatisfacción de Lingel por algunos de los métodos empleados en la investigación sobre Hartmann.

Las alegaciones contra Lingel ponían de manifiesto las diferencias fundamentales entre la filosofía policial europea y la estadounidense. Europa tiende a rechazar las operaciones encubiertas por arriesgadas y cuestionables desde la óptica moral y jurídica. Estados Unidos, por el contrario, recurre a ellas de forma habitual, y en el país existe un intenso debate sobre los límites entre operación encubierta e incitación al delito. En Europa, algunos sectores de la policía consideraban que la operación de Dark Market se hallaba en la frontera entre ambas, sobre todo en el caso del Servicio Secreto, que según parece alentó a los miembros de la web a cometer delitos (en el caso de Dron) en el transcurso de la investigación. El FBI y Keith Mularski defendían a toda costa su forma de proceder. Recalcaban que, gracias a la presencia de Keith Mularski y su equipo en Dark Market, se había recabado la información

necesaria —relativa sobre todo a los planes de expansión de Cha0— para evitar pérdidas potenciales por valor de setenta millones de dólares.

Cuando ya estaba dando los últimos retoques a su reportaje radiofónico sobre aquel peculiar pero importante caso, Kai Laufen sufrió una hernia discal. Incapaz casi de moverse, el periodista se vio obligado a guardar cama dos semanas. Durante ese tiempo llegó a la conclusión de que a nadie en Alemania iba a importarle que el FBI hubiera dado caza a un tarjetero alemán ni que él, Kai, hubiera descubierto la identidad del agente. Por otra parte, el caso de Dark Market había despertado una atención considerable en la prensa especializada de Estados Unidos. Liderados por la revista *Wired* de San Francisco, numerosos medios habían publicado artículos sobre el asunto, sobre todo a partir del espectacular secuestro de Mert Ortaç en abril de ese mismo año y la posterior detención de Cha0 en septiembre.

Kai se sentía en el deber de difundir las pruebas de que Dark Market era en parte una operación encubierta del FBI. Pero de la misma manera que el Atlántico marca la frontera entre dos culturas policiales, el océano separa también los patrones éticos de los periodistas alemanes y de sus colegas angloamericanos. (La policía de Gran Bretaña es más europea que estadounidense, pero sus gacetilleros tienen aún menos escrúpulos que los de Estados Unidos).

En Alemania se considera mala praxis publicar el nombre completo de presuntos delincuentes en proceso de juicio, y en muchos casos los medios del país renuncian a hacerlo incluso cuando su culpabilidad ha sido probada. Lo mismo ocurre con los agentes encubiertos. Naturalmente, si uno está acostumbrado a los medios angloamericanos, esa clase de reparos le parecen inconcebibles.

Así pues, a principios de octubre de 2008 Kai Laufen contactó por teléfono con Kevin Poulsen, el editor de la sección de seguridad de la revista *Wired*, y le informó de que podía proporcionarle pruebas documentales que demostraban que las fuerzas de la ley habían estado infiltradas en Dark Market. Estaba dispuesto a incluir el correo en el que Mularski admitía ser Master Splyntr, pero solo con la condición de que Poulsen no publicara el nombre del agente. Para incidir en esto último, Laufen terminó el correo en el que enviaba los documentos escaneados con el exhorto: «¡Quemar después de leer!».

Poulsen recuerda el capítulo de forma distinta: por lo visto, solo se comprometió a ocultar el nombre de Matrix. A lo largo de años, él y su equipo habían realizado una labor magnífica cubriendo multitud de casos de

delincuencia informática, incluido el de Dark Market. En realidad, no hacía más que aplicar a su trabajo el mismo celo que en el pasado había demostrado como *hacker*, ocupación que lo había llevado a los tribunales. Evidentemente, Poulsen leyó pero no quemó. El 13 de octubre se publicó la noticia. Para Master Splyntr, aquello equivalía a una sentencia de muerte.

Keith Mularski montó en cólera cuando vio su nombre publicado en *Wired*; en un instante, había perdido la confianza ganada a pulso entre los tarjeteros. Un par de semanas antes había cerrado los foros de Dark Market porque el dominio de JiLsi estaba a punto de expirar. Si Master Splyntr hubiera intentado renovarlo, cualquier *hacker* informado podría haber aprovechado la oportunidad para desvelar su identidad.

La operación Dark Market era la fase inicial de un plan a largo plazo de la policía para infiltrarse en el mundo de la delincuencia informática. Durante los quince meses anteriores a la aparición del nombre de Mularski en la revista *Wired*, el FBI, la SOCA y las demás fuerzas policiales implicadas habían identificado a miembros sueltos. Se había excluido la posibilidad de una operación a gran escala, como la del Servicio Secreto contra Shadow Crew en 2004. La intención de Master Splyntr era volver a la carga con su reputación intacta, armado con su amplia base de datos de los tarjeteros y sus actividades. Ahora su plan se había venido abajo.

De todos modos, los esfuerzos de Mularski no habían caído en saco roto: en un llamativo ejemplo de colaboración supranacional entre distintos cuerpos policiales, se había conseguido atrapar a Cha0, uno de los peces gordos del mundo de las tarjetas, y arrestar a docenas de otros, algunos de los cuales ya estaban cumpliendo condena o a la espera de juicio.

En cualquier caso, ni el agente Mularski ni nadie podía culpar a Dietmar Lingel. Contrariamente a lo que afirmaba el Dezernat 3.5, Lingel no había filtrado la identidad de Master Splyntr para que figurase en los documentos del caso de Matrix.

Dicho honor le correspondía al detective Frank Eissmann, el jefe de Lingel, quien más tarde confesaría haber cometido «una grave equivocación» al ceder el documento a la fiscalía del Estado como parte de las pruebas policiales contra Matrix. Fue la equivocación de Eissmann la que permitió que Kai Laufen identificase a Mularski, lo que a su vez supuso el desplome de la operación a largo plazo contra los tarjeteros.

Dietmar Lingel, no obstante, siguió suspendido y no tuvo noticias de sus superiores hasta que el Dezernat 3.5 le informó, en septiembre de 2010, de que se celebraría un juicio. La fiscalía había desestimado la tesis de que

Lingel hubiera podido filtrar el nombre de Mularski de forma voluntaria y había recuperado los cargos del primer momento: se lo acusaba de haber informado a un sospechoso de que se hallaba bajo vigilancia.

Lingel optó por impugnar los cargos. Algo más tarde ese mismo mes dio comienzo en Stuttgart el juicio más largo de todos los relacionados con el caso Dark Market. Irónicamente, entre las partes no figuraba ningún ciberladrón (a excepción de Matrix001 y Fake, que comparecieron en calidad de testigos), sino la desacreditada policía de Baden-Württemberg y uno de sus agentes. Fue un proceso fascinante, celebrado ante un reducido número de personas en un pequeño, pulcro y anónimo juzgado de Bad Cannstatt, el distrito de los balnearios de Stuttgart. El testimonio de casi una docena de actores del drama fue alarmante y revelador de los muchos errores e infortunios que habían jalonado la operación tanto en Europa como en Estados Unidos.

38

¿QUIÉN ERES TÚ?

Estambul, octubre de 2008

Çağatay Evyapan parecía tranquilo en su celda. De vez en cuando, algún miembro de la policía de Estambul murmuraba algo acerca de un superagente que vendría desde Ankara para hacerse cargo del interrogatorio de Çağatay. En Turquía, el tiempo máximo que se puede retener a un sospechoso de pertenencia a banda organizada son cuatro días. El prisionero estaba impaciente por ver si el gran hombre de la capital iba a presentarse.

Finalmente, apareció el inspector Şen. Solo necesitaba saber una cosa.

«¿Quién es el pajarito? ¿Con quién te comunicas? Es lo único que quiero saber de ti».

El prisionero, con gesto atribulado, vaciló.

«No hay nadie».

39

DE CAMINO A NINGUNA PARTE

El trabajo del inspector Şen había concluido. Tras la detención, el caso pasaba a manos de la fiscalía, según dicta la ley turca. Pero si Çağatay Evyapan era Cha0, ¿quién era entonces Şahin, la persona que según Mert Ortaç era el auténtico Cha0? ¿Era Şahin un simple producto de la imaginación de Mert? Al fin y al cabo, Mert tenía un nutrido historial en materia de fantasías y exageraciones.

Pese a su tendencia a la fabulación, la historia de Mert era cierta en sus aspectos fundamentales. Trabajó, efectivamente, para varias organizaciones, entre ellas la Agencia Nacional de Inteligencia; poseía grandes dotes de programación, sobre todo en lo que se refiere a la decodificación de tarjetas inteligentes; amasó grandes sumas de dinero vendiendo tarjetas de Digiturk falsas, motivo por el que se le abrió una investigación; intentó impresionar a la gente organizando fiestas y derrochando dinero; frecuentó los foros de Dark Market con las cuentas de Sadun, Cryptos y PilotM; fue de vacaciones con su novia al hotel Adam & Eve de Antalya, y fue secuestrado y humillado por Çağatay Evyapan.

Sin embargo, nunca pudo aportar pruebas de que Cha0 fuera en realidad el misterioso Şahin. Mert demostró tener un conocimiento tan detallado del funcionamiento interno de Dark Market que, si mentía, alguna organización o alguien debía haberle facilitado toda o parte de la información de que disponía al respecto. La pregunta —para la que todavía no hay respuesta— es: ¿por qué? ¿A quién trataban de engañar o desacreditar involucrando al extraordinario Mert Ortaç? Evidentemente no a Çağatay Evyapan, que en el relato de Mert desempeña un papel secundario. ¿A la policía? ¿O quizá a la persona que, según Mert, se ocultaba tras Lord Cyric, uno de los pesos pesados de la red en Turquía y en el mundo entero?

La versión de Mert no es menos plausible que la del inspector Şen. La clave no está en la identidad de Şahin o Çağatay, sino en el personaje de Cha0. No cabe duda de que la persona que ideó la fábrica de clonadoras y actuó como administrador de Dark Market fue Çağatay Evyapan. La cuestión

es si era Çağatay quien controlaba toda la operación o si trabajaba por cuenta de una organización criminal más importante.

La policía turca detuvo a un total de dos docenas de personas que, a tenor de las pruebas, estaban conectadas con la operación de Cha0, de forma directa o tangencial. El delincuente virtual no era más que eso: no una persona real, sino una amalgama de individuos con diferentes habilidades trabajando en grupo. Tiempo atrás, el fundador ucraniano de Carder Planet, Script, ya había reconocido que bajo el término genérico *tarjetero* se congregaban muchos perfiles distintos: *hackers*; diseñadores gráficos; ingenieros electrónicos que ensamblaban las clonadoras; personas que las instalaban en los cajeros; otras que extraían el dinero; otras que se encargaban de la seguridad, y otras que se dedicaban a reunir información, ya fuera para los delincuentes, ya para la policía.

Tanto Cha0 como Script, pues, anticiparon cómo sería el mundo de la delincuencia informática después de Dark Market: dejó de ser una comunidad de individuos más o menos asociados con el fin de perpetrar delitos puntuales para convertirse en organizaciones criminales más sistemáticas en las que cada miembro realizaba una función específica: envío de correo basura, programación de virus, blanqueo de dinero, gestión de *botnets* y demás actividades propias de la delincuencia virtual.

Por lo tanto, es posible que Cha0 no fuera sino una operación: una forma de reunirlo todo bajo un solo nombre. Cha0 era un nombre colectivo cuyo objetivo consistía, en primer lugar, en hacerse al menos con el monopolio parcial de la nueva industria del fraude con tarjetas de crédito clonadas. Era un plan audaz y habría tenido éxito de no haber sido por el trabajo en equipo de Keith Mularski y Bilal Şen, así como por el apoyo de otros cuerpos policiales y alguna que otra persona a título individual.

El grado de organización de Cha0 como entidad apunta también otro cambio. Hasta fecha reciente, las hermandades criminales tradicionales «tendían a considerar a los delincuentes informáticos como ciudadanos de segunda clase», según palabras de uno de los ciberpolicías más destacados de la SOCA. Sin embargo, durante la existencia de Dark Market, los cuerpos policiales de todo el mundo empezaron a observar que sus investigaciones cibernéticas conducían de forma inesperada a bandas del crimen organizado.

Dentro de Dark Market, podían distinguirse tres núcleos bien definidos. El primero lo componían los administradores, moderadores y demás miembros con altos cargos «burocráticos». En su mayoría, procedían del entorno *hacker* y contaban con conocimientos informáticos avanzados. Con la excepción de

Cha0, sus beneficios no eran cuantiosos y algunos trabajaban directamente para la policía o como confidentes.

El segundo núcleo comprendía a delincuentes hábiles y experimentados que en su mayoría trabajaban por cuenta propia, como Freddybb y RedBrigade. El grado de competencia informática variaba de uno a otro. Pero, en todo caso, si no sabían cómo resolver un problema, sí sabían a quién recurrir. Los miembros de esta clase participaban en los foros de Dark Market con menor frecuencia que los administradores y su equipo. Su objetivo era ganar tanto dinero como fuera posible sin llamar la atención, aunque en ocasiones también opinaban y bromeaban sobre la comunidad tarjetera en general.

El tercer núcleo estaba formado por delincuentes con un alto grado de profesionalidad, gente prácticamente invisible sobre la que circulaban leyendas tanto entre sus colegas como entre la policía. La actividad de estos iba más allá incluso de la venta al por mayor de tarjetas de crédito y *malware*; un ejemplo sería el ucraniano Maksik, detenido por la brigada telemática turca en Antalya en 2007. El más famoso de todos (de quien se dice que suministraba a Maksik buena parte de su material) es el ruso conocido simplemente como Sim, que según la policía podría ser otro grupo organizado. Los miembros de esta categoría nunca emergen de las sombras.

El caso de Cha0 resultaba crucial y fascinante porque era la primera vez que un perfil que imitaba la estructura de las bandas tradicionales llevaba a cabo operaciones a gran escala y trataba de condicionar el funcionamiento de una web como Dark Market. Aquella fue la primera prueba de que la delincuencia informática no era coto tan solo de ciudadanos de segunda clase, sino que empezaba a atraer a figuras más influyentes.

El crimen organizado tiene una fuerte raigambre en Turquía. Las bandas turcas, por ejemplo, controlan el tráfico de heroína hacia Europa occidental con la ayuda de grupos kurdos y de los Balcanes.

A finales de 1996, un Mercedes blindado protagonizó un espectacular accidente de tráfico en la pequeña localidad de Susurluk. Entre los fallecidos se encontraban el jefe de la academia de policía y el líder del grupo terrorista Lobos Grises, incluido en la lista de los más buscados de Interpol por tratarse de uno de los mayores traficantes de heroína de Europa, amén de un reconocido asesino. El único superviviente fue un diputado del partido por entonces en el poder.

El accidente fue el disparo de salida para que periodistas y oposición empezaran a desenmarañar la red de violentos engaños que relacionaba al

Estado Profundo con los miembros más influyentes de ciertos grupos del crimen organizado. Durante años habían intercambiado amistad, hospitalidad y protección. La noticia pilló por sorpresa a la ciudadanía turca y dio un impulso significativo a las fuerzas políticas emergentes del país, como la plataforma que terminaría convirtiéndose en el AKP, que hizo bandera de su lucha contra el crimen y la corrupción.

El país ha avanzado bastante desde entonces. Pero, cuando las raíces de la corrupción y el crimen organizado son tan profundas como en Turquía en los años ochenta y noventa, se necesitan décadas para erradicarlas del tejido político. Esto explica los temores de Bilal Şen al saber que tal vez Cha0 contaba con la protección de poderosas figuras de la clase dirigente. Podría ser también que, como creen algunos de los colaboradores de Bilal de fuera de Turquía, el Cha0 de Dark Market estuviera integrado en una organización de mucha mayor envergadura. Las organizaciones criminales turcas tocan distintos palos: además del tráfico de heroína, Turquía es un importante centro de tráfico de personas (una vez más, por su proximidad a la Unión Europea), y en las dos últimas décadas también el volumen de negocio del blanqueo de capitales ha aumentado.

De ser así, Çağatay Evyapan no sería más que el lugarteniente del auténtico presidente del *holding* criminal llamado Cha0. Çağatay sería el vicepresidente de la división telemática, y no le importaría volver a ingresar en prisión, porque, en términos metafóricos, estaría «interceptando una bala dirigida a su jefe». Tal vez Şahin sea el presidente de la compañía. En ese caso, el Şahin de Mert sería real y el inspector Şen no habría dado todavía con su hombre.

Dark Market fue clausurado en octubre de 2008, pero nadie —ni policía ni delincuentes— tiene la menor idea de cuál es su verdadera historia ni cuál ha sido su verdadera importancia. Han pasado tres años y solo unos pocos de los casi cien detenidos en todo el mundo han pasado a disposición judicial.

Los sistemas jurídicos se están encontrando con un sinfín de dificultades para enfrentarse a la naturaleza altamente tecnológica de las pruebas relativas a la delincuencia informática, y el hecho de que la mayoría de los delitos se cometan en terceros países representa un gran escollo a la hora de detectarlos y perseguirlos. Ambigüedades, dudas, falsedades y disimulos siempre han formado parte del modo de actuar del crimen organizado. Internet no ha hecho más que magnificar su poder.

40

EL EXPRESO DE MEDIODÍA

Prisión de Tekirdağ, oeste de Turquía, marzo de 2011

Un hombre vagamente apuesto vestido con un elegante traje negro y corbata a juego me escrutó mientras entraba en la pequeña sala oblonga. Sus ojos negros y la amplia frente acentuaban su mirada hipnótica y, por un momento, me quedé mudo. Ahí estaba el hombre sobre el que tanto había leído, hablado y pensado a lo largo de casi dos años. Y ahora que por fin lo conocía, no se me ocurría qué decir.

Llevaba dos años y medio encerrado en prisión, pero no había perdido un ápice de distinción y autocontrol. Durante las tres horas que duró nuestra entrevista, pude percatarme de que intentaba sonsacarme tanto como yo a él.

Mi primera visita a Tekirdağ había tenido lugar en 1976, justo antes de la publicación del libro *Expreso de medianoche*, que más tarde Alan Parker convertiría en película de éxito. El libro narra la historia de Bill Hayes, un joven estadounidense que es detenido por intentar sacar droga de Turquía de contrabando. Su espantoso suplicio a manos de un sádico funcionario de prisiones conmocionó al público europeo y norteamericano. Turquía, por entonces, tenía fama de país brutal e implacable. De hecho, durante mi visita, fui atacado, mientras dormía en una tienda de campaña, por un grupo de matones que gritaban consignas contra los extranjeros.

Treinta y cinco años más tarde, volvía a la prisión de Tekirdağ. Como en el caso de Bill Hayes, se trataba de una instalación de máxima seguridad. Situada a un kilómetro y medio por una ladera de inclinación moderada, en los alrededores solo había campos yermos hasta donde alcanzaba la vista. A través del velo tupido que formaba la espesa nieve, acerté a ver los altos muros de desvaído color crema de la prisión y las torres de vigilancia, en cuyo interior se distinguía la silueta de los centinelas armados con ametralladoras. Mi primera impresión fue que nada había cambiado desde la película de Parker.

Una vez dentro, no obstante, me alivió saber que en aquella parte del país al menos las condiciones penitenciarias habían mejorado hasta el punto de resultar irreconocibles. Todos los reclusos disponían de televisor, ducha y aseo en la celda. La comida era más bien espartana, pero sin duda nutritiva y razonablemente sabrosa, en tanto que los celadores se comportaban con cortesía, no solo hacia mí, sino también hacia los presos. En más de un aspecto, las condiciones eran preferibles a las de muchas prisiones británicas.

Había en Tekirdağ algunos reclusos notables, entre ellos el instigador de la muerte de Hrant Dink, el escritor armenio asesinado por unos extremistas sin más motivo que ese, ser un escritor armenio. Tampoco era de extrañar que en la prisión estuvieran también algunos de los principales señores de la droga de Turquía.

Entre los distintos terroristas y capos mafiosos, había un representante de la más reciente variedad delictiva: la delincuencia informática. Tardé más de un año en conseguir audiencia con Çağatay Evyapan: tuve que convencer tanto a las autoridades turcas como al propio Evyapan. Durante meses, pareció del todo imposible. Apenas pude disimular mi estupor cuando, un lunes de principios de marzo de 2011, recibí un mensaje de la Dirección de Prisiones de Ankara en el que se me informaba que, si Çağatay convenía en ello, se me permitiría verlo aquel mismo miércoles. Después, continuaba el mensaje, Çağatay sería trasladado y no volvería a haber otra ocasión.

Lo que las autoridades turcas no sabían, y de saberlo les habría traído sin cuidado, era que mi pasaporte se hallaba perdido en algún rincón de la sección consular de la embajada china de Londres, a la espera de visado. Mis intentos de recuperar el pasaporte para volar a Estambul el martes fueron automáticamente rechazados por los funcionarios chinos. Llamé a la prisión de Tekirdağ y solicité posponer la entrevista un día. Me informaron que, si recibían la orden de trasladar a Cha0 antes del jueves, no se me permitiría verlo bajo ningún concepto. La búsqueda habría terminado.

Se comprenderá, pues, mi impaciencia durante el trayecto de Estambul a Tekirdağ a través de la tormenta de nieve el jueves por la mañana, con un día de retraso. Era muy posible que al llegar me dijeran que había perdido la oportunidad de reunirme con Cha0. Tras una larga espera, me condujeron a través de tres puertas giratorias de acero que se abrían colocando la mano en un lector biométrico y me presentaron al alcaide. Lejos de ser un ogro, como yo esperaba, era un hombre encantador y afable. Me dijo que no habían recibido ninguna orden de Ankara y que después de almorzar en la cantina podría hablar con el señor Evyapan.

Finalmente, me condujeron hasta la pequeña sala oblonga. Çağatay Evyapan es cauto pero seguro de sí mismo. Bilal Şen me había advertido que, si mi intención era obtener información mediante añagazas, su instinto lo detectaría al instante. Me recordó a Julian Assange, el cerebro de Wikileaks: un tipo con una perspicacia portentosa y, a la vez, convencido de su propia superioridad intelectual, cosa que en ocasiones puede confundirse con un extremo narcisismo.

Cuando le sugerí que Lord Cyric era Tony —el tipo rechoncho con gafas mencionado por Mert Ortaç—, resopló con supremo desprecio. «Ha hablado con la inteligencia turca, ¿verdad?», me espetó. En cierto sentido, Cha0 tenía razón: si Mert mentía (que, admitámoslo, era posible), el tipo de las gafas tenía que ser un añadido del MİT, la inteligencia turca.

Durante la charla, Çağatay me confirmó algunos puntos importantes de la historia de Mert, como la situación del apartamento donde fue secuestrado y los intercambios de mensajes entre este y Lucy Hoover, la funcionaria de la embajada estadounidense. También admitió que lo habían detenido por culpa de un error cometido en el mundo real.

A pesar de su inteligencia, Cha0 confesó tener un gran miedo, que irónicamente resultó ser el mismo que el de su más acérrimo enemigo en la policía turca. Según Çağatay, en el momento de interrogarlo, uno de los agentes lo había invitado a acogerse al programa de protección de testigos. A cambio, debería testificar en la investigación de Ergenekon. Lo que le pedían era que admitiera haber creado, por cuenta del Estado Profundo, una red virtual secreta entre el ejército, los servicios de inteligencia y los medios. La policía niega de plano haberle hecho tal oferta.

Cha0 rehusó. Como el inspector Şen, lo último que quería era verse arrollado por la lucha entre el Estado Profundo y el gobierno. En el ciberespacio las cosas funcionan de otra manera.

A lo largo de nuestra charla, Çağatay sugirió que él y un reducido grupo de *hackers* poseían un conocimiento mucho mayor de las cosas que se estaban cociendo en el lado oscuro de la red que ningún cuerpo policial. Con esto quería dar a entender que su intención tan solo era demostrar la futilidad de los intentos de las fuerzas de la ley y el orden por controlar internet; en su opinión, siempre irán a la zaga de personas como él.

Curiosamente, el hecho de estar en prisión y la posibilidad de tener que cumplir los veintidós años de su anterior condena del año 2000 parecían traerlo sin cuidado. Y eso a falta de saber qué cargos se presentarían contra él por su actividad en Dark Market.

Al atacar el asunto del FBI y Keith Mularski, su rostro adquirió poco a poco una expresión mordaz. «El FBI no tiene nada contra mí. Si así fuera, ¿por qué Master Splyntr no ha enviado información que la policía turca pudiera utilizar en mi contra? —preguntó—. Lo único que pueden hacer es manipular al pelele de Ortaç para intentar tenderme una trampa». A continuación, Çağatay afirmó haber pirateado la base de datos de Mularski y haberse hecho con la información reunida por el FBI sobre los miembros de Dark Market, él incluido.

Por supuesto, desde la cárcel Çağatay no podía documentar sus afirmaciones. Aseguró que desde el principio había sabido que Splyntr era del FBI (a pesar de que Çağatay ingresó en Dark Market a invitación de JiLsi en febrero de 2006, fecha en que Master Splyntr ya estaba bien establecido en los foros) y que su estrategia consistía en «mantener a los amigos cerca y a los enemigos todavía más cerca», de ahí su voluntad de colaborar con Master Splyntr en la administración de la página.

Parecía un buen momento para poner fin a la charla. En definitiva, la de Dark Market es la historia de dos hombres, Çağatay Evyapan y Keith Mularski, cada uno con su equipo y sus contactos. Cha0 no era un delincuente ordinario. A pesar de que su objetivo prioritario era ganar dinero, Çağatay parecía convencido de que la lucha entre él y las fuerzas del orden revestía un significado más profundo, como si tratara de demostrar su superioridad técnica y, por consiguiente, la inutilidad de los intentos de las fuerzas de la ley por controlar el ciberespacio. En eso se dejaba ver con fuerza el anarquismo original de la cultura *geek*: los patrones de conducta y los códigos morales cambian cuando pasamos de lo real a lo virtual. Las reglas del juego son distintas y nuevas.

El agente del FBI había obtenido la victoria, pero por poco y ni mucho menos de forma definitiva. Tres años después de la clausura de Dark Market los ecos de aquella extraordinaria empresa criminal siguen resonando por prisiones y juzgados de distintos lugares del mundo. Y, por supuesto, son muchos los exmiembros de Dark Market que todavía rondan el ciberespacio.

Internet es un invento trascendental que se ha extendido hasta el último rincón de nuestras vidas y hasta la última habitación de nuestros hogares. Pero cuidado: Lord Cyric podría estar escondido en algún armario virtual.

EPÍLOGO

A primera vista, la desaparición de Dark Market parecía propinar un golpe mortal a la delincuencia en internet. Mas no fue así. Sí sirvió para paralizar temporalmente el negocio de algunas de las grandes redes de tarjeteros, como las de Cha0 en Turquía, Maksik en Ucrania y Freddybb en Inglaterra. Para los demás delincuentes informáticos, el mensaje estaba bien claro: formar parte de foros de tarjeteros como Shadow Crew y Dark Market, sobre todo los de lengua inglesa con nutridas nóminas de miembros, entrañaba un grado de riesgo inasumible.

Algunas pruebas apuntaban ya que a los miembros de Dark Market, a diferencia de a los de Shadow Crew, les interesaba menos labrarse una reputación que ganar dinero. El número de mensajes colgados por gente como Freddybb disminuyó de forma radical de una web a otra. En Shadow Crew, llegó a enviar cincuenta mensajes públicos y doscientos privados; en Dark Market, quince y doce respectivamente. El desmantelamiento de Shadow Crew a manos del Servicio Secreto estadounidense demostraba de forma inequívoca la vulnerabilidad de esa clase de páginas, y Freddybb aprendió la lección: mejor pasar desapercibido.

En cualquier caso, aparte del riesgo de detención, los foros de tarjeteros habían perdido su utilidad primigenia. Durante casi un decenio de actividad, los delincuentes se habían servido de esas páginas para crear redes globales con personas de confianza. A esas alturas, tanto compradores como vendedores de datos y documentos obtenidos por vía ilegal tenían ya sus mercados.

Pero lo que sin duda aceleró la desaparición de los foros de tarjeteros fue la noticia de que Keith Mularski era Master Splyntr y la revelación de que Dark Market era en parte una operación policial encubierta. Aquello truncaba la estrategia a largo plazo del FBI y sus socios de Europa occidental, cuyo plan consistía en que Master Splyntr reapareciera en el papel del tarjetero honrado que había conseguido burlar al FBI y que, por ello, merecía todavía más la confianza de la hermandad tarjetera.

Después del caso Dark Market, *hackers*, *crackers* y delincuentes informáticos han pasado a estratos más profundos de clandestinidad digital y el negocio ha experimentado una creciente especialización. *Hackers* y programadores de *malware* desarrollan programas diseñados para sistemas específicos o enfocados a buscar un tipo de información muy determinada. Luego los venden a los grupos que supervisan los ataques contra las instituciones financieras o sus clientes. Cuando han conseguido acceder al dinero, contactan con un «mulero», es decir, alguien para quien trabajan «mulas financieras» en distintos lugares del mundo. En la red son incontables los anuncios en los que se ofrece trabajar desde casa con el ordenador. Algunos son obra de muleros. En ellos, le piden a la potencial mula que ponga sus cuentas bancarias a su disposición a cambio de un porcentaje de las sumas que circularán a través de ellas.

Esta atomización de la actividad criminal dificulta que las fuerzas de la ley averigüen qué operaciones tienen lugar y quién colabora con quién. La proliferación de dispositivos y aplicaciones móviles multiplica asimismo las oportunidades de los ciberdelincuentes.

La rápida expansión de internet plantea otro gran problema. Las policías de Europa occidental han notado que el tamaño de la comunidad *hacker* china aumenta a un ritmo frenético. Hasta hace poco, la estafa 419, o fraude del cargo anticipado, era prerrogativa de los grupos criminales de África occidental, principalmente de Nigeria, que fue donde se idearon esos mensajes de correo estrambóticos en los cuales se requiere al destinatario que ayude a mover varios millones de dólares pertenecientes a un dictador fallecido.

La estafa 419, que toma su nombre de un párrafo del código penal nigeriano, es un truco muy viejo; de hecho, el modelo se halla ya en *El alquimista*, una comedia del dramaturgo isabelino Ben Jonson. Básicamente, el estafador convence a su víctima de que le adelante una pequeña suma de dinero, prometiéndole que más tarde percibirá una cantidad mucho mayor. Después, una de dos: sigue exprimiendo a la víctima o desaparece sin más con el primer depósito. En tiempos isabelinos ya era posible, pero resultaba laborioso. Sin embargo, gracias a internet se ha convertido en un negocio muy lucrativo, ya que, por medio de los correos basura, los estafadores pueden acceder a un público de decenas de millones de personas, lo que multiplica las oportunidades de pescar a algún primo.

Hay estafas 419 de todo tipo y para todos los públicos. En ocasiones llegan en forma de apelación dirigida a los ricos ciudadanos de Occidente

para que ayuden a un pobre niño africano. También son frecuentes las cartas, faxes y correos electrónicos en los que se suplica, sobre todo a los norteamericanos, que donen fondos para erigir una nueva iglesia o patrocinar una congregación; en casos así, las víctimas se mueven por un impulso bienintencionado y caritativo. Otra presa para los estafadores del 419 son los enamorados, en especial viudas y divorciadas de mediana edad que entablan relaciones con jóvenes de África occidental, que poco a poco les chupan los ahorros a cuenta de unos escarceos sexuales que nunca llegan a producirse.

Hoy en día, las estafas 419 proceden de China y están escritas tanto en chino como en inglés. El fraude suele ser un complemento de otra de las especialidades de los *hackers* chinos: el robo de artículos en MMORPG (tortuosas siglas para un tortuoso nombre: juegos de rol multijugador masivo en línea) como *World of Warcraft* o los juegos de «reales» como *Second Life* o *Habbo Hotel*. Todos estos juegos funcionan con dinero digital que puede convertirse en dinero auténtico, lo que a su vez confiere valor a los bienes y servicios virtuales, que los jugadores pueden adquirir para mejorar su experiencia del juego. Aunque no son los únicos, los *hackers* chinos han aprendido a «robar» artículos y dinero digital para convertirlo en dinero real. El tremendo potencial informático de China sigue en buena medida sin explotar, a pesar de que en muchos sectores relacionados con la seguridad informática de ámbito civil y militar se considera que es el segundo país en la jerarquía global, por detrás de Estados Unidos. A medida que China descubra sus posibilidades, la naturaleza de internet se irá modificando.

Para combatir estas crecientes amenazas, los gobiernos y la industria destinan hoy en día cientos de miles de millones de dólares a la seguridad informática, ya sea a través de medidas policiales, de la protección de la propiedad intelectual o en el terreno militar. Casi todos esos fondos se invierten en tecnología, con la idea de mantener la red limpia de códigos maliciosos, *malware* y virus que merodean por el ciberespacio a la búsqueda de redes desprotegidas que atacar.

Por el contrario, apenas se invierte en intentar determinar quién piratea y por qué. Nadie distingue entre los *hackers* de Wikileaks, los de los ejércitos estadounidense o chino, los de las organizaciones criminales y los simples curiosos.

Y sin embargo, los *hackers* son una raza extraña y muy particular. Su perfil psicológico y social difiere, en general, de los de los delincuentes tradicionales —sobre todo el de aquellos cuyo papel resulta clave para abrir oportunidades de negocio ilícitas en la red pero no sienten gran interés por el

dinero—; en otras palabras: son *geeks*. Comprender sus capacidades y motivaciones a la hora de cometer determinadas acciones sería de gran beneficio para una industria de la seguridad dependiente en exceso de las soluciones técnicas. En las raras ocasiones en que las fuerzas de la ley o el sector privado siguen la pista de un *hacker* hasta conseguir su procesamiento y condena, casi nunca se trata de comprender al malhechor. En vez de ello, los sistemas penales de Europa y Estados Unidos intentan imponerle duras sentencias de prisión y restringir su acceso a los ordenadores.

Habida cuenta de su peculiar perfil psicosocial, se trata de un gran error. En primer lugar, habría que tener en cuenta la edad: la mayoría de los *hackers* son muy jóvenes cuando se introducen en actividades calificables, al menos, de ambiguas desde la óptica jurídica. Al igual que Detlef Hartmann, pueden sentirse tentados de cometer acciones ilegales en la red antes de que su brújula moral haya evolucionado del todo y sin tener una idea muy clara de las consecuencias de sus actos.

En la vida real, a menudo son personas psicológicamente vulnerables, lo que significa que encerrarlos con criminales de verdad puede ser muy contraproducente, como en el caso de Max Vision. Si bien su ego es imprevisible, todo el mundo concuerda en que posee un cerebro superdotado y unos conocimientos sin parangón en materia de ciberseguridad. En un mundo en que los especialistas en seguridad informática escasean y en que las amenazas son cada vez más numerosas, parece una insensatez confinar en la cárcel a quien podría ser un fenomenal aliado. No estoy afirmando que los *hackers* que hayan delinquido no deban ser castigados, sino que la necesidad de la rehabilitación no es tan solo un imperativo moral del Estado, sino un valor práctico en potencia.

Raoul Chiesa, antiguo *hacker*, dirige un pequeño centro académico conocido como Hacker Profiling Unit, con sede en Turín y financiación de Naciones Unidas. Su investigación se basa en su hondo conocimiento de la comunidad *hacker* y en las respuestas de los *hackers* a los cuestionarios que les envía. Los primeros resultados de su trabajo dan pistas importantes sobre la identidad del colectivo.

Lo más llamativo es la desigualdad entre sexos que domina no solo en la parte ilegal de la red, sino también en la organización y la gestión de internet en su conjunto. Este punto apenas se trata en las páginas del presente libro, pero merece un estudio más detallado. Si en todo el mundo los hombres dominan todavía la política y la economía, su predominio alcanza niveles extremos en lo que se refiere a las nuevas tecnologías. Por supuesto, hay

mujeres muy activas en el terreno de las nuevas tecnologías y los nuevos medios, pero en términos estadísticos no representan más que un pequeño porcentaje: según Chiesa, solo un cinco por ciento. Los *hackers* son, casi invariablemente, hombres.

Un segundo hallazgo del estudio de Chiesa es que el *hacker* tipo es inteligente o muy inteligente. Además, se demuestra que muchos de ellos, casi el cien por cien, poseen conocimientos avanzados en ciencias: física, matemáticas y química. Por el contrario, demuestran un nivel de competencia más bien bajo en humanidades.

Queda, por último, el crucial asunto de las relaciones entre *hackers*. La mayor parte de los *hackers* —pero no todos— se sienten más cómodos estableciendo relaciones en el entorno impersonal de la red que en la vida real. Lo interesante aquí es el porqué.

Lo habitual es que los *hackers* se introduzcan en el mundillo cuando son adolescentes, a una edad en que la mayoría de las personas encuentran dificultades para trabar relaciones, sobre todo con el sexo opuesto; de modo que, al menos en parte, sus dificultades en ese terreno son del todo normales. Sin embargo, Chiesa ha descubierto que un número enorme de *hackers* admiten tener problemas para comunicarse con la familia, en especial con los padres.

La lectura del estudio de Chiesa y mis propias entrevistas con distintos tipos de *hackers* me hicieron acordarme de Simon Baron-Cohen, profesor de Psicopatología del Desarrollo en la Universidad de Cambridge. Su labor pionera en el campo del autismo ha conducido a una comprensión más profunda de los patrones de conducta del espectro masculino/femenino. En general, los varones típicos muestran una mayor capacidad para «sistematizar» el mundo exterior, mientras que las mujeres tienen más facilidad para «empatizar». Esto no quiere decir que las mujeres no sepan leer los mapas y que los hombres no sepan escuchar; implica tan solo que existe una marcada tendencia en un sexo (el masculino) a la «sistematización» y en el otro (el femenino) a la «empatía».

En investigaciones posteriores, Baron-Cohen ha descubierto un nexo entre las mentalidades extremadamente masculinas, que en ciertos casos podrían calificarse de «autistas», y los fetos que quedan expuestos a elevados niveles de testosterona en el vientre materno. Se trata de una tesis controvertida, pero en muchos aspectos convincente y, sin duda, valiosa a la hora de estudiar a los *hackers* y sus patrones de conducta. No todos los *hackers* son autistas, desde luego; de hecho, muy pocos lo son (aunque a algunos de los más

conocidos, como Gary McKinnon, en busca y captura en Estados Unidos por piratear la red del Pentágono, se les haya diagnosticado el síndrome de Asperger).

Si la investigación sigue adelante, quizá en el futuro será posible detectar rasgos de la personalidad de los *hackers* entre los niños en edad escolar. De ese modo, compañeros y mentores podrían ayudarlos a potenciar sus habilidades y, a la vez, facilitarles directrices éticas para que canalizasen sus capacidades en la dirección adecuada. La palabra *hacker* suele tener connotaciones peyorativas, pero en realidad los conocimientos de estos individuos son un activo personal y social. Los ordenadores y las redes nunca serán seguros sin la protección de *hackers* expertos. Algunos ya trabajan en esa dirección. Según mi experiencia, el 90 por ciento de los *hackers* involucrados en actos delictivos expresan fuertes deseos de trabajar dentro de la industria de la seguridad legal; aunque sobre ellos pesen condenas, debería dárseles la oportunidad de hacerlo.

Adewale Taiwo, alias Freddybb

El 1 de enero de 2009, el Tribunal de la Corona de Hull condenó a Adewale Taiwo a cuatro años de encarcelamiento por conspiración con ánimo de estafa entre junio de 2004 y febrero de 2008. En noviembre del año anterior ya se había declarado culpable de uno de los cargos y había admitido la sustracción de algo menos de seiscientas mil libras de cuentas corrientes de distintos países. El juez recomendó que, al término de la sentencia, fuese deportado a Nigeria.

Gracias a una reducción de pena por buena conducta, Taiwo debía quedar en libertad el 29 de agosto de 2010. Dos semanas antes había comparecido ante el tribunal de Grimsby, en la otra orilla del estuario de Humber. Se trataba de una vista estipulada por la ley de incautación de bienes ilícitos, una de las pocas reformas sensatas que Tony Blair introdujo en el sistema penal, en virtud de la cual el Estado puede recuperar los bienes obtenidos con malas artes por los criminales. Pese a la seriedad del caso, la sesión terminó convirtiéndose en una comedia bufa. El fiscal había perdido un archivo crucial, lo que produjo una reacción inesperada por parte del juez Graham Robinson, cuyo buen humor inicial no tardó en convertirse en irritación. Anunció que no estaba dispuesto a retrasar la vista, por lo que las partes tendrían que llegar a un acuerdo de forma más o menos inmediata. Eso beneficiaba claramente a Adewale. El juez terminó fijando una cifra algo superior a 53 000 libras, un recorte considerable con respecto a la suma inicial

de 353 067 libras. El reo declaró que se negaba a pagar, lo que suponía que tendría que pasar un año más en prisión. El 7 de abril de 2011 fue deportado a Nigeria. Taiwo fue uno de los personajes más inteligentes de cuantos frecuentaron los foros de tarjeteros, y durante mucho tiempo llevó con éxito una doble vida como ingeniero químico y ciberdelincuente.

Detective sargento Chris Dawson

El sargento Chris Dawson trabajó en el caso de Freddybb con una diligencia fuera de lo común y sacrificó muchas horas libres para asegurarse de que aquel revoltijo de cifras, fechas y detalles tecnológicos resultara comprensible a los legos cuando llegara a los tribunales. Durante uno de los descansos de la vista de incautación de bienes, Dawson creyó oír a Taiwo diciendo: «A la mierda, no pienso pagar». Cuando el juez abandonó la sala, el detective se marchó indignado ante la incompetencia del sistema judicial inglés.

Sigue trabajando como oficial superior de homicidios en Hull.

Dimitri Golubov

Tras ser detenido en Odesa, el *hacker* Dimitri Golubov pasó cinco meses y medio en prisión, durante los cuales fue interrogado por agentes estadounidenses, entre ellos Greg Crabb del Servicio de Inspección Postal. No obstante, a raíz de la intervención de dos diputados ucranianos, un tribunal de Kiev decretó su puesta en libertad y lo exoneró de todos los cargos en 2009.

Golubov, que mide casi un metro noventa y tiene unos ojos de color azul hipnóticos, niega todo vínculo con Script, aunque su versión de los hechos contiene incoherencias y las pruebas digitales que obran en manos de las fuerzas de seguridad estadounidenses indican lo contrario (por ejemplo, datos extraídos del ordenador de Roman Vega en los que se confirma que Script y Golubov eran la misma persona).

Script se esfumó tras su salida de prisión, pero Golubov reapareció con una nueva iniciativa empresarial y de cambio social: el Partido de Internet de Ucrania. Golubov, que sigue residiendo en Odesa, ha elaborado un programa político destinado a combatir la corrupción, la pornografía y el tráfico de drogas a través de internet. Confía en que, en el plazo de diez años, será elegido primer ministro o presidente de Ucrania. Si por el momento esa parece una posibilidad remota, no hay que subestimar su audacia y ambición. El Partido de Internet ha presentado varias docenas de candidatos a las elecciones municipales de Odesa, y aunque hasta ahora solo ha conseguido un

representante, no cabe duda de que el movimiento está ganando fuerza en todo el país.

Lo curioso es que, a pesar de su rígida postura moral con respecto a ciertos delitos, como por ejemplo la pornografía infantil, Golubov ha emprendido una campaña a favor de la liberación de Maksik, el famoso tarjetero, que cumple una condena de treinta años en Turquía.

Roman Vega

Roman Vega permanece en prisión desde su arresto en Nicosia en febrero de 2003. Extraditado a California en junio de 2004 a petición de Estados Unidos, lleva en la cárcel desde entonces, aunque no ha sido juzgado. En el momento de redactar estas líneas, se halla en el Centro de Detención Metropolitano de Brooklyn, un presidio de lo más espartano en las proximidades de la bahía de Gowanus. Durante todo este tiempo, Vega no ha recibido más visitas que las de sus representantes legales.

En agosto de 2007 se celebró una vista presidida por el juez Charles R. Breyer en el Tribunal del Distrito del Norte de California. Fiscalía y defensa se avinieron a firmar una negociación que dejaría en libertad a Vega por haber cumplido ya los cuarenta y seis meses de prisión acordados entre los abogados. Pero, la tarde anterior a su puesta en libertad, un fiscal del Distrito del Este de Nueva York presentó una nueva serie de cargos y solicitó el traslado de Vega a Brooklyn. Los cargos eran, básicamente, los mismos que en California, pero el letrado de la fiscalía de Nueva York presentó su acusación acogiéndose a un estatuto distinto para sortear las leyes que impiden juzgar a alguien dos veces por el mismo delito.

La transcripción de la vista demuestra a las claras que el juez Breyer, hermano de Stephen Breyer, miembro del Tribunal Supremo, sentía vergüenza e indignación por la estratagema utilizada por el fiscal del Distrito del Este de Nueva York. La base para la nueva acusación fue información facilitada por los agentes del Servicio Secreto.

Tras la llegada de Vega a Brooklyn, el Servicio Secreto le ofreció un trato: si testificaba contra Dimitri Golubov y algunos miembros de la clase dirigente ucraniana (no *hackers*, sino importantes figuras políticas), retirarían los cargos. Si se negaba, presentarían nuevas acusaciones archivadas en otros estados de la Unión. No lo dejarían en paz hasta que aceptase colaborar.

Fuera cual fuese su decisión, Vega ya ha pasado en prisión el triple de tiempo que el resto de los condenados por los mismos delitos en Shadow Crew. Sobre él pesan todavía dos casos sin resolver y la amenaza de más en el

futuro. Vega sufre de caries desde hace años y padece dolores constantes que, en ocasiones, le impiden alimentarse de manera adecuada, pero la Oficina de Prisiones y el Cuerpo de Alguaciles se niegan a prestarle asistencia médica.

No está previsto que Vega quede en libertad en el futuro inmediato.

Maksim Kovalchuk, alias Blade

Kovalchuk fue detenido en marzo de 2003 en Tailandia y extraditado a Estados Unidos, donde cumplió cuatro años de prisión. El FBI consintió en negociar un acuerdo y quedó en libertad en 2007, tras lo cual volvió al anonimato en Ucrania. Su liberación por parte del FBI contrasta ostensiblemente con la obstinación del Servicio Secreto en retener a Roman Vega.

Renukanth Subramaniam, alias JiLsi

El 26 de febrero de 2010, Subramaniam se declaró culpable de un cargo de estafa con tarjeta de crédito y cuatro cargos de fraude hipotecario, por los que el juez del Tribunal de la Corona de Blackfriars lo condenó a cuatro años de prisión. En el momento de escribir este libro, se halla recluido en la prisión de Wormwood Scrubs, en el oeste de Londres, por donde han pasado figuras como el compositor *sir* Michael Tippett y Keith Richards, el guitarrista de los Rolling Stones.

Gracias a una reducción de pena por buena conducta, se prevé que Subramaniam quede en libertad en julio de 2012. El grueso de su caso no se refiere a Dark Market, sino al fraude hipotecario. La fiscalía presentó cinco cargos por tal concepto (aunque tres de ellos fueron negados por las instituciones financieras). A pesar de que el fraude hipotecario es de por sí constitutivo de delito, la fiscalía sugirió que existía relación entre las ganancias que Subramaniam obtenía con Dark Market y los fondos con los que pagaba las hipotecas. Subramaniam, por su parte, asegura que no es responsable del pago de las hipotecas, puesto que lo que hacía era pedirlas en nombre de amigos que no habrían podido permitirse solicitarlas a título propio. Además, Subramaniam se halla a la espera del resultado de su juicio de incautación de bienes para saber si debe confiscársele aún más patrimonio. Contra él pesa una orden preventiva, en aplicación de la cual no podrá interactuar con ordenadores sin supervisión durante los cinco años siguientes a su salida de prisión.

Detlef Hartmann, alias Matrix001

El 9 de octubre de 2007, el Tribunal Regional de Stuttgart dictaminó que Hartmann debía ser juzgado por trece casos de fraude con tarjeta de crédito. El mismo tribunal anunció, no obstante, que rechazaba la propuesta de procesamiento por conspiración con ánimo de delinquir. Desestimado el más grave de los cargos, Hartmann salió de la prisión de Stammheim, donde había pasado los cuatro meses anteriores. La clave de la decisión que impidió juzgarlo por conspiración debe buscarse en la interpretación que hizo la sala de la Ley Fundamental alemana, su Constitución, en la que se establece que todo miembro de una conspiración debe formar parte de un «grupo unificado» en el que se presuma «la subordinación del individuo a la voluntad del colectivo». El juez afirmó que la naturaleza fluida de internet y la estructura de afiliación de Dark Market no satisfacían dicho criterio; una decisión que, como es evidente, tiene importantes consecuencias en lo que se refiere a la redacción de leyes relacionadas con la delincuencia en internet en Alemania.

En julio de 2008, Hartmann obtuvo una suspensión condicional de condena de veintiún meses por los cargos de fraude. Desde entonces ha retomado sus estudios de diseño gráfico y se ha desvinculado totalmente de los grupos clandestinos.

RedBrigade

Se halla prácticamente rehabilitado y vive en Europa.

Max Vision, alias Max Butler, alias Iceman

El 12 de febrero de 2010, un tribunal de Pittsburgh condenó a Max Vision a trece años de cárcel, la mayor pena de prisión jamás dictada contra un *hacker* por un tribunal estadounidense. Según los cálculos de la fiscalía, sus operaciones habían provocado pérdidas por valor de más de ochenta y cinco millones de dólares. Actualmente, se halla recluido en la Institución Correccional Federal de Lompoc, en el sur de California, donde no se le permite el acceso a ordenadores de ninguna clase.

Las habilidades de pirateo de Vision no conocen parangón; se trata sin duda de uno de los hombres más inteligentes de cuantos cumplen condena en Estados Unidos. En una entrevista a puerta cerrada en el otoño de 2010, discutí su caso con uno de los máximos responsables de la rama de amenazas cibernéticas del Departamento de Seguridad Nacional. El funcionario convino

conmigo en que tener a un experto informático tan capaz como Vision pudriéndose en prisión era quizá un desperdicio de capital humano, pero señaló también que su ego —casi tan grande como su inteligencia— era otro factor importante a tener en cuenta.

Nicholas Joehle, alias Dron

Joehle ha salido de prisión tras cumplir su condena por fraude con tarjetas de crédito y producción ilegal de máquinas clonadoras.

Hakim B, alias Lord Kaisersose

Lord Kaisersose se encuentra en libertad bajo fianza en Marsella, a la espera de juicio. Francia es otro país en el que convendría engrasar un poco las ruedas de la justicia.

Cha0

Cha0 puede hallarse al frente de su negocio en Eslovenia o en prisión: depende de si Cha0 es en realidad Şahin o Çağatay Evyapan. Este último se encuentra en prisión preventiva en Tekirdağ, uno de los centros penitenciarios más seguros de Turquía. Se prevé que sea juzgado este año, pero el fiscal ha desestimado los cargos más graves de pertenencia a banda organizada.

Mert Ortaç, alias SLayraCkEr

Mert se encontraba en prisión preventiva en una cárcel de Estambul a la espera de juicio por el caso Akbank cuando en marzo de 2010 quedó en libertad gracias a un tecnicismo jurídico. En noviembre de 2010 volvió a ser detenido y, en el momento de redactar estas páginas, sigue en prisión preventiva. De todas las personas implicadas en Dark Market, Mert es una de las más dotadas, pese a su carácter díscolo e imprevisible.

Keith Mularski y Bilal Şen

Siguen patrullando las malas calles del mundo virtual.

Lord Cyric

¿Quién es? La búsqueda continúa…

NOTA SOBRE LAS FUENTES

El grueso de la información contenida en este libro es fruto de unas doscientas horas de entrevistas llevadas a cabo entre 2009 y 2011. Leonida Krushelnycky dedicó también varias horas a la realización de entrevistas.

Además, he recurrido a dos fuentes documentales principales. En primer lugar, las actas judiciales de varios procesos relacionados con los sitios web Carder Planet, Shadow Crew y Dark Market. En segundo término, los archivos de las propias webs, en especial las dos primeras, que siguen disponibles en la red. Por desgracia, el archivo de Dark Market no es tan accesible. Me consta la existencia de una única copia, pero obra en manos del FBI, que, por razones operativas, no está facultado para compartirla.

Existe una cantidad considerable de literatura sobre los temas de la delincuencia telemática, el ciberespionaje industrial y la guerra informática, buena parte de ella en internet. Por su rigor, quisiera destacar el trabajo de Kevin Poulsen y su equipo, cuyo *blog (Threat Level)* está a la vez bien escrito y debidamente documentado. No puedo dejar de recomendar dos libros que abordan de forma específica la delincuencia informática: *Kingpin*, de Kevin Poulsen, y *Fatal System Error*, de Joseph Menn. Para una introducción más amplia a los problemas derivados de la tecnología de internet, la primera parada debería ser *The Future of the Internet: And How to Stop It*, de Jonathan Zittrain.

Otros *blogs* de gran valía son *Krebsonsecurity*, de Brian Krebs; el boletín *Crypto-gram*, de Bruce Schneier; el *blog* de F-Secure, una empresa de seguridad informática finlandesa, y, por último, *Zero Day*, el *blog* de Dancho Chanchev y Ryan Naraine en ZDnet.

AGRADECIMIENTOS

Durante la redacción de este libro me encontré con un buen número de problemas que nunca habría podido superar de no ser por la generosa ayuda que recibí de varios amigos y colegas de distintas partes del mundo.

En Gran Bretaña, dos personas desempeñaron un papel fundamental. Leonida Krushelnycky demostró ser una investigadora infatigable y a menudo descubrió material decisivo cuando yo ya había perdido la esperanza de dar con él. De no ser por sus esfuerzos, el valor de este libro sería considerablemente inferior. Vesna Vucenovic se encargó de que la administración del proyecto fuera lo más llevadera posible.

En mis viajes, tuve la suerte de cruzarme con dos periodistas con una paciencia y una alegría tan grandes como su profesionalidad y su oficio, que son del más alto nivel. Kai Laufen me ayudó a comprender la complejidad de la justicia alemana, pero su contribución fue mayor aún gracias a los contactos que me facilitó y la hospitalidad que me dispensó. De la misma manera, me habría visto del todo perdido en Estambul y Turquía de no ser por Şebnem Arsu. Por su tenacidad, su cortesía a prueba de bomba y su facilidad para hallar soluciones cuando todo parece perdido, estoy en deuda con ella.

Entre los integrantes de las distintas fuerzas de policía de todo el mundo con quienes he discutido el caso Dark Market, debo destacar al agente Keith J. Mularski del FBI, al inspector Bilal Şen del Departamento contra el Contrabando y el Crimen Organizado de la policía turca y al detective sargento Chris Dawson de la policía de Humberside. Los tres dedicaron mucho de su valioso tiempo a iluminarme con su conversación y en todo momento se mostraron dispuestos a aclararme todo cuanto pudiera resultarme confuso. Quisiera dar las gracias también a los agentes de la Agencia contra el Crimen Organizado de Londres y a Christian Aghroum, antiguo miembro de la OCLCTIC de París.

Desde otra perspectiva, RioRita, de Ucrania, ha resultado ser una mina de información acerca de Carder Planet y demás, así que vaya aquí mi agradecimiento. Igualmente, mucho de lo que sé sobre delincuencia

informática se lo debo a RedBrigade. Estoy muy agradecido por su amistad y por el buen talante con que ha acogido mis incontables solicitudes de información y análisis.

Matrix001 y JiLsi se mostraron dispuestos en todo momento a compartir su detallado conocimiento de Dark Market y a asesorarme en ocasiones puntuales. En Pittsburgh, Max Vision resultó ser un interlocutor útil y brillante. A los tres, mi más sincero agradecimiento.

Aunque sus versiones difieran, Çağatay Evyapan y Mert Ortaç son dos de las personas más interesantes que he conocido en los últimos tres años. No quiero dejar de transmitirles mi gratitud a ambos, a pesar de la difícil situación en que se encuentran.

En Estonia, Madis Tüür fue un guía excelente —por no hablar de sus dotes de anfitrión— para conocer la política y la historia del país.

Gracias también a Brooks Decillia de la CBC de Calgary por su desinteresada investigación. De forma parecida, Daniel Goldberg y Linus Larsson acudieron a mi rescate en Estocolmo.

Dos personas me ayudaron desde bastidores con las partes más técnicas: Mikko Hyppönen, jefe de investigación de F-Secure en Helsinki, y Vicente Díaz, de Karspersky Labs en Barcelona, se mostraron dispuestos en todo momento a ayudarme a comprender cosas que no me cabían en la cabeza. Rex Hughes, del Wolfson College de Cambridge, también me dio sabios consejos sobre cuestiones de seguridad informática de tipo más general.

Quisiera dar las gracias también a las siguientes personas, que me ayudaron cada cual a su manera: Allison Culliford, Luke Dembosky, Sophie Devonshire, Joris Evers, el detective Spencer Frizzell, Tamara Glenny, Camino Kavanagh, Suat Kınıklıoğlu, Dirk Kolberg, Darryl Leaning, Melissa Llewelyn Davies, Jane McClellan Q. C., Mark Medish, Steve Milner, Jaan Prisaalu, Colin Robinson, Anya Stiglitz y Eneken Tikk.

Mis agentes y editores me prestaron un apoyo inestimable. Clare Conville, de Londres, es la mejor agente que imaginarse pueda y cuenta con un equipo formidable. Michael Carlisle realiza una labor igual de dinámica desde Nueva York. Tengo la suerte de contar con un trío de editores —Will Sulkin en Bodley Head, Dan Frank en Knopf y Sarah MacLachlan en Anansi Press— que me facilitaron mucho la labor de escritura, a la vez que aportaron considerables mejoras al producto final. Quisiera dar las gracias asimismo a otras dos personas que tuvieron una influencia significativa en el libro: Kay Peddle, de Bodley Head, y Janie Yoon, de Anansi.

Mis tres hijos, a quienes este libro va dedicado, demostraron un sano interés en el proyecto a pesar de mis frecuentes ausencias, físicas y mentales, durante el proceso de su redacción. En ningún momento dejaron de animarme y apoyarme.

Y por último, mi agradecimiento y mi amor para Kirsty Lang, mi esposa, cuyos comentarios, críticas y camelos me ayudaron a mantenerme a flote a lo largo del proceso. No es la primera vez que me salva la vida.

Junio de 2011



Misha Glenny (nacido el 25 de abril de 1958) es un periodista británico multilingüe, especializado en el sureste de Europa, el crimen organizado mundial y la ciberseguridad. Fue educado en Magdalen College School en Oxford y estudió en la Universidad de Bristol y en la Universidad Charles de Praga antes de convertirse en corresponsal en Europa Central de The Guardian y más tarde de la BBC. Se especializó en informar sobre las guerras yugoslavas a principios de los años 90 que siguieron a la desintegración de Yugoslavia. Mientras estuvo en la BBC, Glenny ganó el Sony Gold Award de 1993 por su destacada contribución a la radiodifusión. Publicó tres libros sobre Europa Central y Oriental.

En McMafia (2008), escribió que el crimen organizado internacional podría representar el 15 % del PIB mundial. Glenny asesoró a los EE. UU. Y algunos gobiernos europeos sobre cuestiones de política y durante tres años dirigió una ONG que colaboraba en la reconstrucción de Serbia, la ex República Yugoslava de Macedonia y Kosovo. Glenny apareció en la película documental Raw Opium: Pain, Pleasure, Profits (2011).

Los últimos libros de Glenny continúan su interés en el crimen internacional. DarkMarket (2011) se refiere al cibercrimen y las actividades de los piratas informáticos involucrados en el *phishing* y otras actividades. Némesis: Un hombre y la batalla por Río (2015) sobre el narcotraficante brasileño líder

Antônio Francisco Bonfim Lopes (conocido como Nem) en Rocinha (`Pequeña granja`), una favela (barrio pobre).

Notas

[1] La distinción más sencilla, si bien incompleta, entre virus, gusanos y troyanos, conocidos en conjunto como *malware*, radica en sus vías de transmisión: los virus se contagian a través de archivos infectados remitidos por correo electrónico; los troyanos, a través de las descargas; los gusanos, por su parte, poseen la capacidad de autorreplicarse en un ordenador huésped para después utilizar los programas de comunicación de ese mismo equipo y extenderse a otros. A la postre, todos resultan perjudiciales. <<

[2] Siglas del Massachusetts Institute of Technology; no deben confundirse con las de la Agencia Nacional de Inteligencia de Turquía. **<<**